EUROPEAN UNIVERSITY INSTITUTE

Department of Law

Ambient Intelligence and the right to privacy.
The challenge of Detection Technologies

SHARA MONTELEONE

Thesis submitted for assessment with a view to obtaining the degree of
Master in Comparative, European and International Law (LL.M.) of the
European University Institute

Supervisor: Prof. Giovanni Sartor

Submitted for language correction

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Ai miei genitori, a Bruno e a Novella.

A Ben.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

ABSTRACT

Unprecedented advances in Information Communication Technologies (ICT) and their involvement in most of private and public activities are revolutionizing our daily life and the way we relate to our environment. If, on the one hand, the new developments promise to make people's lives more comfortable or more secure, on the other hand, complex social and legal issues arise, in terms of fundamental rights and freedoms. The objective of this study is to envisage some of the main legal challenges posed by the new Ambient Intelligence technologies (AmI) and in particular by the new security enforcement technologies for privacy and data protection.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Table of contents

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

THE IMPACT OF AMI TECHNOLOGIES ON HUMAN RIGHTS. THE CASE OF *AMBIENT INTELLIGENCE DETECTION SCENARIOS* 39

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

INTRODUCTION

The central questions of this study could be formulated as follows: which (new?) privacy issues have been raised by the recent developments of intelligent computing, especially by those used for security purposes?

It is possible to specify the main questions into the following sub-questions: a) are there any conceptual and legal changes with regard to the right(s) of privacy related to the ICT developments of the last decades? b) Is the current legislation appropriate for covering the new challenges of AmI and which are, possibly, the main enforceability issues? c) What kind of solutions can be suggested (legal – new/old – technical measures, both)? d) What is the European policy on this issue (and in particular, is the adoption of the Lisbon Treaty going to introduce relevant changes)? Finally, a general question could be posed on the role of the Law in a 'democratic society', as it is facing the new technologies threatening for fundamental rights (for instance, should the Law protect the individual against such threats or ignore them?).

After having analyzed the possible applications of AmI technologies and the evolution of the concept of privacy, one main avenues of inquiry in the first chapter will be to consider the adequacy of the current legal regulation models to respond to these new challenges. In the second chapter, attention will be paid to the possible use of these new technologies for security purposes ('detection technologies'), and therefore to the balancing issue between opposed interests and rights according to the principles appropriate for a 'democratic society'. Given the limited scope of this study the focus will be on the European framework, although with a view to other legal (and technological) systems.

If, on the one hand, the new developments promise to make people's lives more comfortable or more secure[1], on the other hand, complex issues arise, in terms of fundamental rights and freedoms - among which, the right to privacy- traditionally protected, although in different ways, by the Constitutions of the EU Member States[2]. In this sense, privacy could also be seen as an example of those fundamental rights that are challenged by new technologies, "the process of which is faster and

[1] Cook. D. - Augusto J. C. *et al.* (2009). Ambient Intelligence: Technologies, applications and opportunities. *Pervasive and Mobile Computing*, 5 (4), 277-298.
[2] Leenes *et al*. (2008) *Constitutional rights and New Technologies*, Asser-Press the Hague.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

more difficult to regulate compared to traditional technologies"[3]. In particular, serious concerns for privacy (and related rights) of the individuals seem to rise from the increasing diffusion of devices allowing the 'mobility' and also the remote identification and control of items, persons and interests, due to their stronger capability to invade into the private sphere and their general 'reluctance' to be subjected to legal restraints[4].

It might be helpful to start this paper with a brief overview of the recent developments in AmI technologies, in order to identify, besides the opportunities they promise, the threats they pose to privacy and data protection right(s), after having briefly considered the doctrinal evolution of the legal concept of privacy and having analyzed the related legal sources. It will be useful, for this purpose, to consider, on the one hand, i) the 'adequacy' of the legal principles and requirements, acknowledged by the European Data Protection Regulation, to ensure legal safeguards for individuals (enforceable in Courts) and, on the other hand, ii) their practical applicability: a basic requirement of the Data Protection Regulation, the consent, is difficult or even impossible to be put in practice in AmI environments, where sophisticated technologies operate often without the subject's intervention.

Since the main legal concerns about privacy and data protection arise from the use of new technologies for purposes that may conflict with those of privacy (for example, in order to protect free speech, marketing or security aims), it is worth considering the legitimacy and the necessity of these kind of measures as well as their proportionality according to the current legal framework (particularly, Human Rights Law and EU Data Protection Law) and their jurisprudential interpretation.

In exploring the main current European Regulation, a short account of the legal grounds granted to privacy protection by the Lisbon Treaty will be given (e.g., the binding value of the Charter of Fundamental Rights of Nice). Finally, the paper aims to contribute to the debate on the opportunity to achieve a legislative reform in the field and, possibly, on the criteria to be adopted for balancing privacy and other 'opposed' rights (e.g. security)

[3] Boisson de Chazournes L. (2009). New Technologies, the precautionary principle and public participation, in Marphy T. (ed) *New technologies and Human Rights*, Oxford, Oxford University Press, p. 160.
[4] Dix, A. (2005). Le tecniche Rfid in G. Rasi (ed) *Innovazioni tecnologiche e privacy*. Rome, Ufficio grafico dell'Istituto Poligrafico e Zecca dello Stato, p. 54.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

CHAPTER I

THE AMBIENT INTELLIGENT (AMI) ENVIRONMENT. OPPORTUNITIES AND LEGAL ISSUES

1. Living in an AmI environment

1. 1. The AmI applications

When the computer revolution started some decades ago, probably nobody could expect that the capabilities and intelligence, only imagined in science fiction films, would become a reality. Technologies, which were used until now in a passive way, are becoming active and personalized in order to respond to individual specific needs or desires: we are going towards a world where people are surrounded by easy-to-use interfaces embedded in everyday objects, capable of responding to individuals in a seamless, unobtrusive and invisible way[5].

The expressions Ambient Intelligence, or ubiquitous or pervasive computing, created by computer-science researchers around the world, indicate a quite recent discipline that, taking the advantage of important changes in the Information Communication Technologies, aims at bringing 'intelligence' to our everyday life environments, making them responsive and sensitive to us[6]. More commonly, these terms essentially mean the same thing: "a digital environment that proactively, but sensibly, supports people in their daily lives"[7]. Based on the use of sensors networks,

[5] Wright D. - Gurtwirth, S. *et al.* (2008). *Safeguards in a world in Ambient Intelligence*, London, Springer.
[6] Aarts, E. - Marzano, S. (2003). *The New Everyday. Views on Ambient Intelligence*. Rotterdam: 010 Publishers.
[7] Cook *et al.* 2009, *cit*. p. 278.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

wireless communications, smart devices (with the miniaturization of microprocessors), the central idea of AmI is, firstly, to reduce the dimension of computers, so that they can be embedded in familiar objects (mobile phones, GPS navigator, home equipments); secondly, to employ the augmented computation capacity and the spreading availability of the devices – technology distributed around us –in order to provide a mixed, real-virtual experience that 'should' improve the way we can benefit from our surroundings.

While we are becoming accustomed to sensors that control temperature or lighting in modern houses, the possibilities of Ambient Intelligence go much further than that, allowing the combination more than one electronic device in order to interact in an 'intelligent' way with the users, that is, to be adaptive and responsive to features, behaviour and acts of users, thus providing personalized services and anticipating their needs. The legal relevance of these technologies, their invasive nature and the fact that they rely on the collection and processing of personal data make privacy right safeguards and Data Protection Regulation are, therefore, undoubtedly applicable. What is more difficult to say is to what extent and in which manner they should be applied.

Though it is impossible to refer to all the studies devoted to the development of Ambient Intelligence in this paper, it could be useful to underline some of their main features, especially those related to the privacy issues discussed in this paper[8]. The *sensing* capability of AmI allows the interaction between technology and the real world and relies on a variety of sensors employed. Environment and user's characteristics are *perceived* by a software algorithm that uses these data to *reason* and *act* consequently in order to change the environment. Thus, the development of profiling and personalization algorithms is crucial for the success of an AmI system[9]. It is possible to argue that, as long as the perception of movements, temperature, position, pressure remains anonymous (in the sense that the system doesn't need to identify a specific person in order to operate), relevant legal issues of privacy and data protection are not raised, at least, not directly.

The problem is that tracking, locating and identifying specific people in a certain environment (i.e., on the basis of their features, devices or other distinctive means) has become essential in the new AmI systems, in order to provide services

[8] These features are: *sensing, reasoning and acting,* as identified by Cook *et al*. (2009) *cit*. p. 278.
[9] De Vries (2010). K., *Identity, profiling algorithms and a world of ambient intelligence*, Ethics and Information Technology, 12 (1), 71-85.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

according to the situations, needs and preferences of different users. Tracking people and items is performed, for example, by using technological measures (such as Radio Frequency Identification -Rfid- tags) that require individuals and items to be 'tagged'[10], that is, to be continuously followed, monitored, guided, with consequences in terms of invasion of private life and profiling, especially if they are combined with other technological measures (motion sensors, cameras, microphones, unique identification number). Profiling in itself is not forbidden by current EU legislation. The legitimacy of the profiling activity is, nevertheless, defined by specific legal requirements (in particular, lawfulness and limited finality). The increasing use of Rfid for different applications (logistics, access control, etc.), due to the cost reduction of computing and communications, which will facilitate exchanges of information among smart and small devices, shows that we are already living in an AmI world.

As it has been argued, AmI will directly affect our lives in many ways, as individuals, as professionals and as citizen. Accordingly, safeguards for privacy-related rights (i.e. anonymity, identity, non-discrimination and non-manipulation etc.) should be ensured in various situations of the individual, whether they are private or public. Broader considerations of the current society should be taken into account in order to properly address all the issues raised by these technologies and before they become ubiquitous. Besides the invisibility, accessibility and other technical innovations, attention should be paid to the increasing concerns for security after 11 September 2001 (hereinafter 9/11) and to the weakening of public control on this development[11].

Further developments in computer science, which are going to surpass the limits of the existing technologies (i.e. to ensure a proper and exact identification of people, to avoid imprecision and failure of sensors perception[12]) together with the convergence of different media and different systems, are making the situation more complex and worrying for several reasons. First, the existence of blurred concepts in the current EU Data Protection Regulation (such as that of 'personal information') renders its application difficult in practice. Moreover, identifying people with their precise names or addresses is becoming needless, since, in order to create a profile and to provide customized services, it may be sufficient to know, in some cases, only the identification number of their computer device, while in others, namely the

[10] *Ibid.*
[11] Wright *et al.* (2008), *cit.* p. 74.
[12] See Cook *et al.* (2009) *cit.* p. 279

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

categories to which a person is likely to belong[13]. Furthermore and foremost, the increasing use of biometric data (fingerprints, but also eye retina or smell)[14], for both security and non-security purposes (that sharpens the issue of conflict between rights) guarantees an exact identification of the individual involved.

In order to be adaptive and act unobtrusively but in an appropriate way (e.g. completing a task when it is supposed to be needed by the subject that interacts with the system[15]), an AmI system needs to work well in terms of reasoning capability, the features of which are extremely relevant in privacy-related debates. For example, the ability to model users' behaviour, to predict and recognize activities in the environment, the ability of decision-making on behalf of the individuals based on their profile settings, are aspects that clash with some of the main principles of privacy and Data Protection (as discussed later, necessity, finality, data minimization, proportionality), leaving aside the relative ethical and social considerations [16].

The scientific literature regarding the advances of technologies in this context is quite rich even if only few applications of AmI projects have been yet fully implemented. A broad overview of the different projects developed in Europe (as well as in the rest of the world, particularly in the U.S.A. and in Japan) is illustrated in the SWAMI report[17]. Within it, also a first example of Ambient Intelligence "vision" promoted by the European Union and commissioned in 2000 to the Information Society Technologies Advisory Group (ISTAG). This vision has constituted the basis for the following research agenda within and without Europe alike.

The scenarios for possible applications and activities that these technologies are expected to provide are manifold and involve private as well as public spaces. Some examples are the smart homes (e.g. for the intake of proper food), hospitals (for the intake of medicines/health monitoring and assistance), transportation (for increased safety, e.g. controlling the driver's behaviour), smart office or campus (for information services or use of remote facilities). First of all, it is essential for the

[13] D. Wright *et al.* (2009). Privacy, trust and policy-making: challenges and responses. *Computer Law and Security Review*, 25 (1), 69-83.
[14] New applications of biometrics have been discussed at the International Computer Privacy and Data Protection Conference (CPDP), Bruxelles, 29-30/01/2010.
[15] Simpson *et al.* (2006) Plans and Planning in Smart homes, in J. Augusto - C. Nugent. *Designing Smart Homes*. *The role of Artificial Intelligence*, London, Springer-Verlag.
[16] See G. T. Marx, (2001) Technology and Social Control in N. Smalser- P. Baltes (eds) International Encyclopedia of the social and behavioral Science, Oxford, Elsevier.
[17] Wright *et al.* (2008), *cit.*, 47.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

AmI system, in order to function appropriately, to be aware of the subject's preferences, intentions, and needs in order to 'act' automatically (that is to anticipate, interrupt or suggest to the subject). The AmI system will rely on a human-computer interaction (using intuitive interfaces), which nowadays includes voice, facial and emotion recognition. In this framework, the computers will actually be everywhere, invisibly integrated in everyday items and more autonomous from a direct input of the subject.

It is easy to imagine how this bears upon the effectiveness of legal preconditions of data protection such as the previous consent and the information obligation. With this aim, some projects tried to verify the enforceability of these requirements through the design of *ad hoc* technical tools (such as the "privacy agent" software)[18], which is able to provide automated consent for the processing of personal data). Recently, the European Data Protection Supervisor adopted an Opinion on the usefulness of "privacy by design", which is considered a key tool to ensure a citizen's trust in ICT[19].

It is possible to identify some main threats to privacy and related rights on the basis of the different components of an AmI system: hardware, pervasive wireless communications between computers, intuitive interfaces, embedded intelligence controlling interfaces and communications or due to unauthorized access thereto[20]. Ubiquitous communications imply the wireless transmission of a large amount of data. In this case the reduction and the encryption of data transmitted could be used as safeguards - a task that could be performed automatically, according to the principle of necessity and depending on the purpose of the communication. Doubts about the possibility to achieve anonymity derive from the increasing use of unique identifiers (IP addresses, Bluetooth device ID, RFID tags), enabling the tracking of communications between devices (embedded into personal items) and users.

---

[18] Le Metayer D. - Monteleone S. (2009). Automated consent through privacy agents: legal requirements and technical architecture. *Computer Law and Security Review*, 25 (2), 136-144.

[19] See D. Le Metayer (2010) Privacy by design: a matter of choice in S. Gutwirth, Y. Poullet, P. De Hert (eds.), *Data Protection in a Profiled World*, Springer Verlag, p. 323: "the general philosophy of privacy by design is that privacy should not be treated as an afterthought but rather as a first-class requirement in the design of IT systems: in other words designers should have privacy in mind from the start when they define the features and architecture of a system"; see also the EDPS Opinion (2010) on Promoting Trust in the Information Society by fostering Data Protection and privacy, available at:
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf.

[20] The main problem deriving from hardware components is their miniaturization (becoming difficult to be noticed and easy to lose or steal, with the relevant risks for the data stored in it). The centralized storage of data is considered risky and unlawful regarding the protection of privacy, due to the possibility of combining data gathered from other parts of the system: see Wright *et al.* (2008), *cit.* 71.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Future developments require, therefore, better protection mechanisms. Advanced interfaces would be able to interpret the users movements, face features and emotions so that the 'embedded intelligence' could reason about how to use the personal data gathered (providing suggestions or acting autonomously on behalf of the user). The main concerns for the user's privacy seem to derive from the lack of control on the logging of the interactions, the possibility they are accessed by an unauthorized person, as well as the undue use of sensors (fake biometrics or identity theft).

Some solutions to these counterfeits would be to charge the embedded intelligence with the task automatically to select the privacy policy appropriate for the particular context in which it is used and to minimize the relative use of data. Also, to adopt security systems that allow continuous recognition of the owner of a specific device (unobtrusive but reliable biometrics, more user-friendly than a password or PIN codes) or to permit the user easily to switch off functions when he/she wants [21].

1.2. The increasing use of social control technologies

The amount of data collected by cameras and biometric systems through the use of automated devices and their 'intelligent' use in order to provide personalized services, clearly, gives rise, as mentioned above, to privacy and data protection problems. In particular, collection, storage, processing of communication and diffusion are activities legally acknowledged according to the European Data Protection Regulation, which establishes their minimum limits and requirements, regardless of the technologies employed in practice. Furthermore, the invasive nature of some technological solutions gives rise to compliance issues with regard to traditional privacy principles, such as proportionality or the 'purpose limitation' that

[21] S. Gutwirth, (2007) Biometrics between opacity and transparency, *Annuali dell'Istituto superiore di Sanità*, 43 (1), 61-65. Another interesting aspect (impossible fully to cover in this paper) concerns the reliability and security of the system that should be normally addressed by encryption techniques. These techniques are difficult to use in an AmI context because they run counter to the principle of minimal resources, which is typical of such technologies. The risks of technical errors and the misleading capacity of the system could also affect the protection of individual privacy and some of the existing projects are focused on that disadvantage, for example designing specific devices in order to secure the information transmission or to be able to preserve location data private, or to employ biometrics in order to ensure privacy See: E. Vildjiounaite - S.M Makea, *et al.* (2006). Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices, in *Pervasive Computing*, Proceedings of the 4th International Conference, PERVASIVE 2006, Dublin, Ireland, May 7-10, 2006. Berlin-Heidelberg: Springer.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

are set in international conventions concerning the protection of Human Rights, particularly the European Convention of Human Rights (see *infra*).

Although the afore-mentioned features of AmI are presented by scientists as a way to make surroundings more adaptive and helpful for the users (e.g., reducing the individual's efforts in performing certain tasks), or even to address important challenges such as environmental protection, health care or transportation[22], the same AmI advocates could not avoid taking into account the privacy concerns and indeed, they became more responsive towards them[23].

This paper necessarily focuses on the legal aspects of these technological advances, even though we cannot disregard completely some of the socio-political issues at stake, which also have legal implications[24].

G.T. Marx, in particular, warns about the increasing use of science and technology for acquiring social control. "The control has become softer and less visible, partly because it is built-in…partly because of the more sophisticated use of deception" and it became, according to him, more extensive (by, e.g., blurring traditional institutional and organizational borders) and more intensive (by, e.g., passing the boundaries of distance and darkness or by breaking physical barriers – factors that traditionally protected liberty and privacy).

According to G.T. Marx, the increase of social control via engineering is related, on one side, "to concerns over issues such as crimes, terrorism, border control, economic competitiveness…", and on the other, "to the technical developments in electronics, computerization, artificial intelligence[…]; paradoxically increased expectation and protection of privacy have furthered reliance on external, distance-mediated, secondary technical means, that identify, register, classify, validate or generate grounds for suspicion". Marx is convinced that we should assure the control of technology rather than the reverse. This assumption appears relevant also for the success of the legal-technical approach, which is

[22] See the OECD Experts Conference, (2009) Using Sensor-based Networks to address Global Issues: Policy opportunities and Challenges, Lisbon, 8-9 June 2009.
[23] D. J. Cook (2009), *cit*. See also the Opinion of EDPS on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes (2010/C 47/02) of the 22/07/2009.
[24] G. T. Marx (2001); D. Lyon (2007). *Surveillance studies, an overview*. Cambridge, Polity.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

currently quite popular among European jurists and scientists in the general debate on data protection[25].

Especially after 09/11, security and predictability trends seem to have increased dramatically in our society, in parallel with the (less diffused) fear of witnessing the realization of a total-surveillance society, a sort of Bentham's/ Foucault's 'Panopticon', several times denounced by legal-sociologists[26]. The use of GPS in mobile phones and other location-aware services, for business or governmental security purposes, although presenting many benefits, have raised concerns amongst privacy advocates as far as the risks of unwanted and unwarranted surveillance are concerned. These risks are doomed to increase in a world of AmI, where intelligent devices will be able easily to detect people, places, movements. This is probably a challenge for the legislative authorities, which have to ensure that proper safeguards are adopted in order to avoid the unauthorized and abusive access to the data collected, especially in the frame of a blurring private and public distinction[27]. Among others, Rouvroy [28] critically evaluates this strong emphasis that modern societies put on security and prevention issues, that seems drastically to erode the protection of the right to privacy, especially when it is combined with the use of invasive technologies.

2. Privacy and data protection. Concepts and legal categories

Before discussing the particular emphasis now paid to security interests, as reflected in the recent adoption of legal security measures by several International and European Institutions, it is appropriate to consider briefly the concept and the right of privacy itself. It will be sufficient to evoke here the main values founding the privacy right(s) as they can be deduced by the main legal rules aiming at protecting it/them.

The legal literature focusing on privacy issues is very broad, but not yet necessarily elucidative, as far as the exact definition or the expansion of this right, as

[25] Poullet, Y. (2005a). *Comment règuler la protection des données? Réflexions sur l'internormativité*, in P. Delnoy, *Liber amicorum*, Larcier, 2005, p. 1075.
[26] Lyon, D. - Zureik, E. (1996). *Computer, Surveillance and privacy*. Minneapolis: University of Minnesota Press.
[27] See Wright *et al.* (2008), *cit*. 65.
[28] A. Rouvroy, (2008) Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence*, Studies in Ethics, Law, and Technology*, 108 (2),116-122.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

defined by the legal texts (national and supranational) is concerned. Some juridical interpretations have been given by the national Constitutional or European Courts[29], and by opinions and assessments made by the administrative entities set for the regulation and protection of this right (National and European Data Protection Authorities), but they haven't been of much assistance in clarifying the normative content of the right.

The beginning of a legal debate on privacy as an autonomous right of the individual is traditionally ascribed to the North American doctrine developed at the end of the nineteenth century (following the publication of Warren and Brandeis' well known article, 'The right to privacy')[30]. At that time, it corresponded to what later became its essential but not exclusive component, the "right to be let alone", that is, the right to protect the confidentiality of one's private sphere against public or private interferences. From that moment on, the concept and the right of privacy have undergone a significant evolution, due to the socio-economic developments and, much more, due to the introduction of the Information Communications Technologies (ICT) into daily life.

With the development of the Information Society, and the increasing flow of information across the national boundaries, the main focus, especially of the EU regulative approach (*infra*) has become the protection of personal data, considered even more important than the protection of a *strictu sensu* privacy right. Data Protection legislation has introduced a more dynamic dimension of privacy that gives to the citizens/users of communications the right to control the use of their personal information in the modern Information Society. Often used as synonymous terms, privacy and data protection are, therefore, different concepts, (as confirmed by the different legal grounds in the Charter of Fundamental Rights of the EU, *infra*), but, since their relative domains are blurring, it is not possible to recognize two distinct, autonomous rights. In my view, they could be illustrated as circles, sometimes concentric, somtimes intersecting.

The lack of a wider regulation of privacy right(s) and the almost exclusive attention to the issues concerning data protection has been regarded as one of the limits posed by the communitarian approach[31], on the grounds that it would put too

[29] Sudre, F. (2005). La "construction" par le Juge européen du droit au respect de la vie privée, in F. Sudre, *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*. Brussels, Bruylant, p. 11.
[30] Warren S. & L. Brandeis (1890). The Right to Privacy. *Harvard Law Review,* 4 (5).
[31] Lugaresi, N. (2004). Protezione della privacy e protezione dei dati personali: i limiti dell'approccio comunitario, Giustizia amministrativa n. 03/2004. Rome: Istituto poligrafico e Zecca dello Stato.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

much importance on the economic aspect of privacy (personal data seen as a valuable and negotiable or merchandized matter), thus overshadowing other components of privacy, for example solitude, the intimacy of personal relationships, not being under constant surveillance, self-determination and autonomous choice. According to the sustainers of this view, data protection alone wouldn't satisfy all the expectations of a subject's privacy, the latter being also functional for the protection of other individual and social rights[32]. In particular, as highlighted by some American scholars, informational privacy would grant collective benefits, through the promotion of decisional autonomy and deliberative democracy[33].

For this reason, although Europe could boast of a general legal framework on Data Protection (missing in the United States of America) and stronger juridical safeguards, it does not yet seem to have found a meaningful answer to the fact that privacy is a "conceptual muddle" . As underlined by Keats Citron and Henry[34], without a deep understanding of privacy "decision-makers will have great difficulty identifying, defining and protecting against socially detrimental incursions on privacy". It may be enough to think about law enforcement agencies supplying our digital data to marketing companies or about governments accessing our social-network profiles, in order to comprehend the dangers involved for the individual's autonomy.

2.1. A (new) pluralistic conception of privacy

Among other *understandings* of privacy, one particularly interesting is that provided by Daniel Solove[35], who criticizes all the scholars' attempts to choose a common denominator of privacy, as too narrow or too broad, with the risk of creating a privacy conception which is either over-inclusive or too vague and thus unable to respond to important privacy problems. He suggests, therefore, to "understand privacy as a set of family resemblances, not reducible to a singular essence." The author offers a pragmatic approach and a pluralistic conception of

[32] Rouvroy, A. (2008). Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence*, Studies in Ethics, Law, and Technology*, 108 (2),116-122.
[33] Cohen, J. E. (2000). Examined Lives: Informational privacy and Subject as Object*, Stanford Law Review*, 52, 1373.
[34] D. Keats Citron & L. M. Henry (2010). Visionary Pragmatism and the value of privacy in the Twenty-first century. *Michigan Law Review*, 108, p. 1107.
[35] See D. Solove (2008), *Understanding Privacy*, Harvard, Harvard University Press.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

privacy (not only in relation to the activities of collection, but more in respect of the processing, storage and dissemination of data), especially useful because it is focused on the specific and concrete problems of privacy, instead of producing a holistic approach to it. Briefly, in Solove's *method*, privacy is a family of interrelated yet distinct things, that is why similar activities could have different privacy implications.

In that frame, what we consider as entitled to privacy protection is *variable,* according to time, values and technologies. This pluralistic and contingent theory of privacy requires, not only a level of *generality* that ensures extensive applicability, but also enough of stability in order to be legally useful, and this could be achieved, in Solove's view, by *focusing* on privacy problems, thus on a taxonomy of activities (that he divides in four non-definitive groups) that the law should guarantee.

From the lesson taught by Solove, we learn also that our concerns for the right to privacy should not overshadow society's interest for privacy protection. The judges and the legislators should balance privacy against other interests in concrete contexts (1) and protect it when it assures the best outcomes for the society (2). The pragmatist view of Solove allows us to recognize a more complete and useful value of privacy, as a bringer of social benefits, like in the case of an invasive police search: in this case there is a societal interest (not only an individual interest) in avoiding unjust searches, the interest in ensuring that police forces will follow a legally justified procedure before conducting invasive searches[36].

As Keats Citron and Henry argue, Solove's societal view of privacy (his "visionary pragmatism") can help legislators and jurists to face technologies of our time in a thorough manner and guide them better in balancing privacy and other legally protected interests. According to Keats Citron and Henry, one way to apply this pragmatic approach is to oblige decision makers, judges and legislators to explain their assessment of the interests they are balancing and the reason why society would benefit from a particular outcome. The adoption of this approach could, for instance, have brought the Italian Tribunal of Milan to a more accurate (and maybe different) argument in the recent and debated sentence on the Google case[37], in which three Google executives have been convicted for data protection

[36] Keats Citron, D. - Henry L. M. (2010), *cit*. p. 1108.
[37] Tribunal of Milan, Criminal Section, judgment n. 1972 of the 24/02/2010.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

crimes, as the consequence of the users' uploading of a video containing sensitive data[38].

Keats Citron and Henry go beyond the Solove's taxonomy and suggest considering not only the privacy values but also the possible harms that its protection may cost, measurable on a case by case basis (e.g., harms from disclosure and harms from seclusion): not an uncritical acceptance of privacy protection but also the consideration of its negative social costs (e.g. a drug user's privacy and her son safety). That way, according to the authors, some control of decision-makers discretion would be better ensured.

Thus, a consideration follows: looking at the violations of those values that the law aims to protect should make privacy both a concept more connected to reality and a less abstract notion that can guarantee the development of the appropriate legal and practical protection. The use of technical solutions, acting *ex ante*, could be more effective than *ex post* balancing in some cases[39]. Additionally, the technological solutions could better address some of the privacy problems described in Solove's taxonomy.

2.2. Identity and 'contextual integrity' in Information Age

Even though they cannot be considered the same, the right to privacy is often also associated, conceptually and legally, with the right to (personal) identity. The latter is understood, on the one hand, as the right to be able to identity oneself in every circumstance and not be forced into doing so (in the Information Society this right is acknowledged via the notions of anonymity and 'pseudonymity'), and, on the other side, as the right not to be misrepresented[40], as the "truth of person", weighable only against a prevalent public or private interest[41]. It can be noted that the meaning of this interest, for the scope of this paper, is connected to the concepts of decisional

[38] Sartor, G. - Viola de Azevedo Cunha, M. (2010). The Italian Google-Case: Privacy, Freedom of Speech and Responsibility for User-Generated Contents, *Social Science Research Network*, Working Papers, from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1604411.
[39] Keats Citron & Henry (2010), *cit.* 1108.
[40] A. Hoikkaanen, - M. Bacigalupo, - R. Compano, - W. Lusoli, - I. Maghiros (2010). New challenges and possible policy options for the regulation of electronic Identity, *Journal of International Commercial Law and Technology*, 5 (1).
[41] Hildebrandt, M. (2005). Privacy and Identity, in E. Claes - A. Duff - S. Gutwirth, *Privacy ad the criminal Law.* Antwerp- Oxford, Intersentia.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

privacy and 'contextual integrity'[42] that should assume more relevance in the AmI debate.

Some kinds of technology affect the capacity of the individuals to control their personal data and their identification. The risk of erroneous processing of personal data is particularly high on the Internet as well as in sophisticated Ambient Intelligence scenarios, because of the possibility that these kinds of technologies have to use personal data and act unobtrusively. In these contexts, one of the main interests of the related subject could be to reinstate the situation correctly, i.e. the *status quo* regarding his/her personal data. However, the risks that the misuses of data can provoke are more serious, as far as identity theft, discrimination, social exclusions or even stigmatization are concerned. The right to privacy becomes therefore, also, an instrument in order to ensure the ability to exercise other fundamental rights and values of a democratic society. Some of the main components of a privacy right are, in fact, the self-determination and the decisional autonomy of the subject in the context of his/her social and political life[43].

It has been argued that it should be taken into account, especially in ICT contexts, where we deal with electronic identity(ies) that the individual's identity has a changeable nature[44]. Therefore, the subject or entity who collects the individual's personal data (even if legitimately) could acquire a significant power over him/her that should be compensated by the acknowledgment of proper safeguards, in order to ensure that the disclosure or use of such data reflects the true identity of people. Recently, the proliferation of Identity Management Systems (IdM) has been promoted in the marketplaces, providing the users with different available digital identification techniques, different identifiers, and different levels of assurance. Nonetheless, this evolution guarantees neither the awareness of how they actually work, nor the ability appropriately to manage them. More and enhanced information about their functioning and about the effects of the related choices seems, therefore, necessary[45].

Conceptually, identity could be considered wider than the concept of privacy, even if, paradoxically, it is being protected by the right to privacy. Indeed, the two main aspects of identity correspond to the two traditional prerogatives of privacy: its

[42] A. Hoikkaanen *et al*. (2010), *cit*. p. 2.
[43] A. Rouvroy, (2008), *cit*. p. 116.This aspect will be discussed again in the chapter II.
[44] G. Buttarelli, (1997). *Banche dati e tutela della riservatezza.* Milano: Giuffrè.
[45] A.Hoikkaanen, *et al.* (2010), *cit*. p. 2.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

defensive and its offensive aspect, freedom and confidentiality[46]. The ensemble of these two aspects justifies the nature of fundamental right of privacy as well as its acknowledgement by the international and European legal instruments.

3. Current regulation and limits

Considering briefly the legal framework in this field, it is opportune to mention those dispositions of the respective international and European texts, that give to privacy and data protection the nature of fundamental right(s), but that are also characterized by some enforceability issues, especially in the context of the new ICT.

Among the International Treaties that protect the right to privacy, we should mention Art 17 of the International Covenant on Civil and Political Rights (ICCPR), Art 8 of the European Convention of Human Rights (ECHR)[47], both protecting the right to private life, and the Convention of the Council of Europe for the protection of individuals with regard to the Automatic Processing of Personal data (No. 108, Strasbourg Convention of 1981). The latter, though being of European origin, can also be ratified by States that do not belong to the Council of Europe[48].

Although not directly contemplated by the ECHR, data protection has been recognized by the European Court of Human Rights as included in the right of privacy *ex* Art 8, as well as restricted on the same grounds (Art 8 (2)): law requirements, necessity, specific purposes (such as public security) and proportionality (the latter is derived from the interpretation of the Court of Strasbourg). This set of safeguards should be taken into account especially in the development of new technologies, which aim to detect objects and people for purposes that cannot always be deemed 'legitimate'. Within the European Union, we should mention the Charter of Fundamental Rights of Nice, which contains two distinctive articles on privacy and data protection: the importance of this Charter has increased especially because of its bounding value after the recent adoption of the Lisbon Treaty (see II Chapter *infra*).

[46] E. Dreyer, (2005). Le respect de la vie privée objet d'un droit fondamental, *Lexis-Nexis Juris-Classeur* 5 (18).
[47] In many of the countries members of the Council of Europe these Conventions are self-executing, that is, they are superior to national law or on par with national Constitutions.
[48] L. Bygrave, (2008). International agreements to protect personal data. in J. B. Rule- G. Greenleaf (ed), *Global Privacy Protection*, Cheltenham, Edwar Elgar Publishing, p. 15-49.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Since the emerging of ICT technologies and in order to integrate the existing and limited privacy regulation (that did not include the private sector, nor the right to access or correct personal data), the European framework has been enriched by several legal acts dedicated to data protection[49]. The Directive 95/46/EC (Data Protection Directive) is, nevertheless, the first EU instrument that contains general binding rules concerning privacy and data protection and that has been implemented (although with discrepancies) by all Member States, even if, at a national level, some of them had adopted domestic legislations aiming at offering data protection to their citizens earlier.

One of the main innovations of this Directive has been the founding of National DP Authorities, with regulatory and control powers, as well as of an advisory group (DP Working Party, so called "Art 29"), with the task of helping in applying data protection rules also to new technologies (for example, Article 29 DP WP on RFID technology, or the Working Document on biometrics).

Multidisciplinary studies have pointed out that some aspects of data protection are not protected by the legal guarantees provided for the privacy right(s), and this would have been the reason for the adoption of a specific European DP regulation[50].

Nevertheless, though we cannot forget that the Single Market is the first objective of the Communitarian Regulation in general, including the DP regulation, and that this would justify the Community's major attention for data protection (economically valuable for marketing and transaction purposes), the right to privacy right nowadays does not seem to be limited to the sole ability to control one's data. On the contrary, it aims at including a wider sphere of the individual's personal behaviours as well as at protecting the "dominion" over the context in which the individual exercises all of his/her fundamental freedoms[51]. This particular asset of the right to privacy is characteristically evident in its clash with the use of the new information technologies.

While privacy protection instruments could be seen as protecting the 'opacity' of the individuals against the interference of private and public powers, the

[49] See the Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications ('e-Privacy' directive) and the Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, so called 'Data Retention' directive.
[50] D.Wright *et al.* (2008). *Safeguards in a world in Ambient Intelligence*, London, Springer.
[51] S. Rodotà, (1997). *Repertorio di fine secolo.* Roma, Laterza.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Data Protection Regulation system has introduced 'transparency tools'[52], which allow a controlled interference with the individual's private autonomy (through the legal acknowledgment of a balancing system and of procedural safeguards).

In spite of its 'young age', the general principles of the DP Directive have been deemed, also in the recent official reviews, as suitable to be applied even to new technologies[53]. Most of these principles are stated in art 6 and 7 of the Directive or are derived by the jurisprudential interpretation of the same directive. They recall and enrich the principles of the ECHR (specific purposes principle; data minimization principle; fair treatment principle; unambiguous consent). Furthermore, the Directive provides for legal requirements and establishes rights and obligations.

Nevertheless, several issues of implementation and efficacy still remain, especially in relation to the development of a hyper-technological world. Two classes of problems could be immediately pointed out with regard to these principles. First of all, at the level of their abstract formulation, their interpretation has not been univocal in the last years, since consequent conflict issues regarding other legal principles (e.g., security purposes) have occurred. Secondly, a thorny issue relates to their concrete implementation, especially in the virtual society of the Internet, as well as, in the new scenarios proposed by AmI technologies, where data protection rules risk being just misled (new threats arise if we consider the growing up of the "Internet of the Things", *infra*).

In this frame a deeper reflection on the current regulatory framework appears to be necessary[54]. The legal analysis developed in the last decade concerning the Data Protection Regulation system has, in particular, underlined the need, on the one hand of improving and extending the context of certain legal notions (such as that of the 'personal data') and, on the other hand, to achieve adequate specificity in the Data Protection Regulation system. Sector-based legislation at the EU level would be valuable, "in order to apply those principles to the specific requirements of the technology in question"[55]. This could prove to be extremely useful as far as the development of AmI technologies is concerned. Indeed, their new possible deployments and their convergence with other technologies and systems could be

[52] See D. Wright *et al.* (2009), *cit.*, p. 69.
[53] See the Communication of the European Commission, COM (2007) 87, on the follow-up of the Work program for better implementation of the Data Protection Directive, COM (2007) 87 final, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf.
[54] D. Wright *et al.* (2009) *cit.* p. 69.
[55] European Commission COM (2007) 87 of the 07 March 2007.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

better managed at a specific rather than a general level mainly related to their functional and not technological aspects.

As discussed in the second chapter, the entry into force of Lisbon Treaty has partly modified the legal context and prepared the ground for a review of the privacy and data protection framework.

3.1. An "Internet of the things" and profiling issues. A need for DP differentiated regulatory regimes?

It has been shrewdly observed that with 'intelligence' embedded everywhere, an "Internet of the things" increases the possibilities for collecting and aggregating data[56]. Similarly, the continuing advances in computing power will increase data-mining and analysis[57]. The collection and processing of profiling-data has been recognized in recent years as a threat to privacy especially when the access to such data is likely for unauthorized persons[58] or when they are communicated to third parties, due to the risks for these data to be used for purposes other than the original ones (breach of the 'limited purpose' principle).

Other concerns could emerge from discriminatory practices, similar to the online dynamic pricing and price discrimination that remain lawful marketing practices unless they are conducted against the will of the subject or in violation of individuals' fundamental rights. In this last case they are considered to be negative discriminations. The same issues and concerns could be raised in the AmI environment, where the possibility to track the users across different contexts, such as workplace, home and entertainment venues is of crucial importance. Therefore in the AmI environment the risk of a possible erosion in the autonomy of the individual is higher as well as his/her right to diversity according to different situations and

[56] For the definition of 'Internet of things', see the Opinion of the EDPS on *Promoting Trust in the Information Society by fostering data protection and privacy* of 18 March 2010, p. 13: "Information produces by RFID tags -for example, product information- may eventually be interconnected into a global network of communication infrastructure. This is usually referred to as the ' Internet of things'. The data protection/privacy questions arise because real word objects may be identified by Rfid tags that in addition to product information may include personal data". See also the Communication from the Commission to the EP, the Council, the EESC and the Commitee of the Regions on Internet of Things – An action plan for Europe (COM (2009) 278) of the 18.06.2009.

[57] See D.Wright *et al.* (2009), *cit*. p. 70.

[58] In this sense data protection coincides with security protection, according to Keats Citron and Henry, (2010), *cit*. p. 1108.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

circumstances[59]. That is probably one of the principal meanings that we should appoint to the right of privacy today.

Though privacy issues related to the Internet are beyond the scope of this paper, relevant connections are nevertheless possible and necessary, not only due to the similarity of some problems online and offline, but because the Information Society is becoming more and more digitalized and a larger amount of data is actually disclosed in the virtual world[60]. Individuals, families and homes are increasingly connected to the Internet and this raises policy concerns in relation to the protection of their identity, privacy and security[61]. The situation is becoming even more complex to define and regulate if we take into account the augmented possibilities of data diffusion offered by the convergence of technologies and media, that consequently blur the boundaries of our offline world (e.g., that of AmI) and online one (the Internet).

Ronald Leenes, considering profiling and 'dataveillance' (surveillance of and through personal data) as pressing issues of Internet today, argues that it is possible (and more useful) to differentiate between several types of 'identifiabilities', depending on the domain in which they occur or on other factors such as their goals, relations, issues and effects[62]. The different kinds of 'identifiability' could raise different concerns that ought to be addressed in a different way by the regulatory regime (i.e., different Data Protection-related obligations and rights, such as consent, information, etc.). These differences are not taken into consideration by the current legal framework but they could benefit from different regulatory regimes and, eventually, create a common ground between the privacy and industrial advocates. Leenes's assumption is also interesting as far as the matter of AmI is concerned, in particular for his reflections regarding what he calls *Recognition-Identifiers* (e.g., a password) and *Classification*-identifiers (referring to the cases individuals are

[59] R. Leenes (2008), *cit*. p. 4.
[60] B. Daskala - I. Maghiros, (2007). *Digital Territories: towards the protection of public and private spaces in a digital and Ambient Intelligence environment*, (IPTS Report), Luxemburg, OPOCE.
[61] Y. Punie, (2005). The future of Ambient Intelligent in Europe: the need for more everyday life in R. Silverstone (ed) *Media, technology and everyday life in Europe: from Information to Communication*. London: Ashgate Publishers Ltd.
[62] In particular, the Author makes a distinction: *Look up indentifiability*, *Recognition Identifiability*- the first using direct identifiers, like names, passport number but also IP address, the second using indirect identifiers, like cookies, passwords, and they work in the context in which they are created- and, moreover, *Classification identifiability* and *Session Identifiability*, the first referring to the case individuals are classified on the basis of preexisting profiles or categories, the second to the technical solutions that allow to track the subject –like the cookies in Internet, being, so, limited to specific context, See R. Leenes, (2008), *cit*. p. 4.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

classified on the basis of preexisting profiles or categories) and for the practical issues surrounding them, such as the possible uses of the derived profiles[63].

The opaqueness of data-processing in AmI due to the ability of the system to capture and process data in an automated and hidden fashion is one of the reasons for its success. What happens if this unawareness extends also to the same kind of unrevealed and unfair practices that are today used on the Internet (such as, behavioural targeting, stereotyping)? Can a legal requirement such as the consent be deemed appropriate and useful in such kind of situations? Therefore, it seems that recognizing the concerns deriving from the use of AmI mechanisms in different contexts could enable us to find different and differentiated data protection rules. Another relevant issue is which form these rules should have, e.g., hard law or soft law.

I wonder if this assumption could bring us to consider the updating of notions such as 'personal data' and 'identifiable person' that are comprised in current legal provisions and are, as mentioned above, quite broad and unclear, necessary in order to 'deconstruct' them. I also wonder if this could be in line with the view that underlines the importance of making technologies, such as those used in AmI, 'relative' depending on the context and people involved (see below).

3.2. Legal requirements and implementation issues

One of the main general principles of privacy and data protection is the 'fair processing' of data (Art 6, DP Directive) that underpins all the other specific requirements. A "decent treatment of people in society" represents a core value of data protection[64], and implies that people know when and for what purposes their data are collected. The 'purpose specification' and 'purpose limitation' principles are essential in the context of privacy and data protection, and their implementation relies on enacted and applied requirements of transparency. In other words, whatever the context (online or offline, the Internet or AmI), the controller (i.e., the subject who, according to the European Directives, decides the scopes and modalities of data-processing) should clearly specify the reasons of the data collection and the modalities of their use. This requirement derives directly from the information

[63] Regarding the profiling activities, see: M. Hildebrand & S. Gurtwirth, (2008) *Profiling the European Citizen*, Springer.
[64] R. Leenes (2008) *cit*. p. 2.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

obligation provided by the DP Directive, the implementation of which is not always achievable in the ICT environment and in particular in AmI scenarios. Despite quite extensive legislation on data protection and (in a minor way) on privacy, there are still practical difficulties in its implementation[65].

Regarding the compliance of the new technologies, including those used in AmI environments, to the legal parameters it appears necessary not only to ensure that the existing legislation is applicable to new mobile services and that it is implemented in an uniform way in all Member States, but also that an appropriate new regulation should be adopted, where necessary[66]. As argued by Hoikkaanen *et al*.[67], it is important to distinguish the contexts and the typology of the data collected in each of them. Consequently, the legislation should be able to take into account this contextualization and identify the different requirements. AmI technologies require policy-making to be more contextual "without jettisoning coherence"[68]. The fact that new technologies are blurring the boundaries between private and public sectors (e.g., working from one's home) makes the protection of privacy more difficult. Whilst the European Court of Human Rights, in this regard, has stated that the protection of private life should also be extended to the professional life [69], this issue is still ambiguous in Europe, as proved by the differentiated jurisprudence decisions of the national Courts and DP Authorities.

In AmI environments where people and items are connected to each other and are always online it will be more difficult to apply the underlying principles of the right to privacy.

Thus, it becomes more and more urgent to adopt a clearer interpretation of the notion of private life and its additional legal protection[70]. An appropriate direction to follow in the DP Regulation system appears to be that of relative and *ad hoc* rules, yet responding to general common grounds. In order to answer to the need of safeguards arising from the emergence of AmI, one approach could be to adopt a system of "micro-policies" (i.e., sector-bases rules), instead of domain policies that could better fit with the specific circumstances, the specific technologies and

[65] As testified, for example, by the Art 29 DP Working Party, Opinion 1/2010 on the concept of "data controller".
[66] See Y. Poullet (2005), *The Internet and private life*, in Kenyon and Richardson, *New dimension of privacy*, Cambridge University Press, p. 65, who affirms the need to renovate the current legislation for a more adequate data protection.
[67] A. Hoikkaanen et al. (2010), *cit*. p. 3.
[68] D.Wright & S. Gutwirth (2009), *cit*.
[69] See the Judgment *Halford v. United Kingdom*, of the 27/05/1997.
[70] D. Wright et al. (2008), *cit*. p. 74.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

individuals. Therefore, it will be a challenge in the future to instantiate a coherent use of these micro-policies[71].

3.3. Contextualizing privacy and other possible responses

Many privacy problems and issues seem to derive from the type of the AmI technology used in practice, from its more or less pervasive character (e.g., video-cameras and biometrics), from its context (airport or home), or from the purposes it serves (e.g., security or entertainment scopes). In general, the most critical aspects seem to be connected, as mentioned above, to the reduced control that the individuals have over their private sphere and personal data, especially if the AmI system allows them to share information with third parties and gives them the capacity to monitor or access the collected data even when such practices are considered to be unlawful. Indeed, such practices clash with the two cornerstones of DP regulation, the principle of consent and the 'purpose limitation'.

Many authors underline the fact that AmI technologies are particularly risky in terms of privacy and data protection, due to their nature and their tendency to collect detailed personal data that are stored and shared[72]. What is to happen then? Do we have to renounce the future technological progress or do we have to totally abandon our privacy concerns[73]?

In the debate among scientists and lawyers, it is interesting to recall here the thesis[74] that affirms the need to customize privacy as any other preference service, on the basis of the context of AmI environments or the features of people. That is to say that privacy should be influenced by the context in which it is adopted.

The advantage of such an approach relies on the reduced detailed personal information that is necessary in order to satisfy the user's needs, inferring the needed data from previously processed and profiled persons[75]. Nevertheless, 'constitutional' doubts stay on the ground with regard to this view, if proper safeguards are not established. One thing is, in my view, the adaptation of privacy preferences to

[71] *Ibid*.
[72] Rodotà, S. (2009). *La vita e le regole, tra diritto e non diritto*. Milano: Feltrinelli; Wright D. (2005)The dark side of AmI. *The Journal of policy, regulation and strategies for Telecommunications* 7(6), 33-51.
[73] Le Metayer, S. Monteleone (2009), *cit*.
[74] A. N. Joinson *et al.* (2006). The role of situational and dispositional variables in online *disclosures*. Paper presented at the Workshop on Privacy, Trust and Identity Issues for Ambient Intelligence. from: http://www.cs.st-andrews.ac.uk/~pst/pti-ai-workshop/programme/joinson-privacy.pdf.
[75] See Cook *et al.* (2009), *cit.*, p. 288.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

contexts and users. Another is to consider privacy rights as a 'package' that could be acquired as other services (and maybe with the option to 'take or leave' it). As stressed elsewhere[76], the latter approach would be more in line with a proprietary view of privacy, which recognizes a contractual nature of the consent to data processing and considers data as objects of transactions[77]. This view has been criticized by many scholars in Europe[78], because it seems to fail to ensure those privacy-related rights, such as the right to take free and autonomous choices, the individual's decisional autonomy, which are considered as essential to a vivid democracy[79].

3.4. A legal-technical approach

As mentioned above, one of the main privacy and data protection issues is the safeguarding of the implementation of the related rules, especially in the context of ICT applications. In order to find possible solutions and based on the presumption that the best data protection could only be achieved by a legal-technical approach[80], some research projects, founded by the EU, have been trying for years, to develop technologies with the ability to enhance the privacy of user (the so-called *Privacy Enhancing Technologies*, P.E.T.), few of which have so far achieved significant results[81]. Acting directly at the level of the technical designs and standards, the aim of these projects is to anticipate the level of privacy protection, in order to produce 'conformed' technologies and to have a regulation from the *inside* rather than from the *outside* of the technologies. The idea is to put in practice what many scholars have been predicting for some years, namely that the solution to technology is technology itself [82].

[76] D. Le Metayer & S. Monteleone, (2009) *cit*. p. 136.
[77] Bibas, S. (1994). A contractual approach to Data Privacy. *Harvard Journal Law and Public Policy* 17, p. 591.
[78] Y. Poullet, (1991). Le fondement du droit à la protection des données nominatives: propriétés ou libertés*, Nouvelles technologies et propriété*. Paris : Thémis; Bianca, C. M. - Busnelli, F. (2007). *La protezione dei dati personali*. Padova, Cedam.
[79] A. Rouvroy, (2008), *cit*. p. 116.
[80] Y. Poullet (2008), *cit*. p. 65. See also S. Monteleone (2008), Data Protection e comunicazioni elettroniche. Necessità di un approccio tecnico-giuridico, in A. Pace, R. Zaccaria, G. De Minico, *Mezzi di comunicazione e riservatezza*, Jovene.
[81] Kosta, E. - Zibushka, J. Scherner, T. -Dumortier J. (2008). Legal considerations on privacy-enhancing Location Based Services using PRIME technology. *Computer Law and Security Report* 24 (2), 139-146.
[82] Poullet (2001). See, about this aspect, Chapter II *infra*.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Though such an approach seems extremely convincing, there are problems to be solved and privacy threats that should be avoided that especially derive from its possible deviations. First comes the issue of transforming legal provisions into technical standards, thus into 'codes', since legal rules are not easily translatable into computer-logical rules. Secondly, the technical ruling (programming) could be considered to be an autonomous rule-making process[83], rendering it therefore difficult to decide which role should be assigned to it, integrating or replacing the traditional law[84]. A third issue derives from automated data-mining and data-analysis, especially when supporting computerized decision-making (that brings us back to the discriminatory profiling as discussed above). Finally, it could be not so trivial to consider the implications of an all-preventive (*ex ante*) approach (which would replace a repressive one) on the values of self-determination and the decisional autonomy of the individual, as an underlying right to privacy.

It can be affirmed that these implications should be taken into account in the development of new AmI scenarios, if it is true that the success of AmI will depend on how secure it can be made, how privacy and other rights of individuals can be protected and how individuals can come to trust the intelligent world that surrounds them[85].

Finally, two main goals should be achieved: to allow the development of new technologies and to ensure the protection of the individuals' rights threatened by them. Research has highlighted the importance of designing technologies for people instead of making people adapt to technology[86]. To this regard, the afore-mentioned technologies inspired by the idea of 'privacy by design', could play a crucial role in its protection[87].

The debate on which legal and/or technical instruments should be adopted for a better implementation of data protection requirements is still open[88]. The Law is,

[83] R. Leenes, B-J. Koops *et al*. (2008). The Authors point out an other relevant aspect: "the use of computer-assisted and computer-executed legal decisions specially in the field of administrative law[…]require to check on the conformity of the resulting program rules with the legal rules and on the constitutional authority underling the technical rule-making process".
[84] Lessing, L. (1999). *The Code and other Laws of cyberspace*. New York, Basic Books.
[85] Friedewald M. - Vildjiounaite, E. *et al.* (2007). Privacy, identity and security in ambient intelligence: a scenario analysis. *Telematics and Informatics*, 24 (1), 15-29; Sartor, G. (2006). Privacy, Reputation and Trust: some implications for Data Protection, *EUI Working Papers*, Law n. 2006/04, Florence, European University Institute.
[86] D. Wright (2009), *cit*. p. 56.
[87] D. Le Métayer, (2010), cit., p. 324. See chapter II *infra* for some reflections on the changes in the legal instruments urged from this new approach claiming that the legal rules should be embodied into the core functionality of the technical devices.
[88] Poullet, Y. (2005c). Comment réguler la protection des données? Réflexions sur l'internormativité, in P. Delnoy, *Liber amicorum*. Bruxelles: Larcier; D.Le Metayer – S. Monteleone (2009), *cit*., p. 136.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

however, expected to play a crucial role in these new technologies, possibly "looking into the future scenarios in order to identify adequate legal responses"[89].

4. Privacy *vs* security issues

One of the possible conflicts between the right to privacy and other rights is the clash between privacy and security. It is possible to find many traces of the increasing attention for public security interests in the current International and European policies. The Convention of Budapest on Cybercrime and the Data Retention Directive 24/2006/EC are some examples[90]. Regarding EU policy, these trends are becoming very 'strategies', as we can observe in several hard and soft law legal documents (e.g., most recently, the Council of the European Union Stockholm Program).

Although the conflict between fundamental rights and security is not new[91], the post 09/11 effects have tremendously sharpened it, especially as far as privacy and data protection are concerned[92]. Some of the counter-terrorism measures already adopted by the U.S. as well as by the EU raised several doubts about their 'constitutional' legitimacy[93] and about the balancing principle as a proper approach to face such a dilemma. Amongst them, particularly interesting, for their possible and predictable connection with AmI scenarios are the new types of detection technologies, the aim of which is to empower the practices of the fight against terrorism. Privacy issues seem to arise both not only from the increasing resort to these mechanisms, during the last decade, but mainly from the invasive character of the new technologies that enables them to penetrate more deeply into the private sphere of the individuals than ever before (e.g., body scanners). Constitutional challenges raised by these detecting technologies are pointed out by Leenes et al.[94],

[89] Fernandez-Barrera, M. *et al.* (2009). *Law and Technology: Looking into the Future*. Florence: European Press Academic Publishing.
[90] Although, the legal basis of this Directive has been found in the ex art 95 of the TEC (as it has been clarified by the ECJ), it was an immediate reaction to the London bombing. See EDPS Opinion on the communication from the Commission to the EP and the Council on an Area of freedom..*cit*.,p. 4.
[91] Zucca L. (2008). *Constitutional Dilemmas*. Oxford: Oxford University Press.
[92] De Hert, P. (2005), Balancing Security and Liberty within the European Human Rights Framework: A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11. *Utrecht Law Review* 1(1), p. 68-96.
[93] Sheinin M. *et al.* (2009). Law and Security. Facing the dilemmas. *EUI working papers Law* 2009/11. Florence, European University Institute.
[94] R. Leenes *et al.* (2008) *cit*. p. 12.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

in particular with respect to the rights to intimacy, inviolability of the body and of the home.

It is not difficult to imagine that the situation could become more thorny with the future development and use of AmI technologies for these purposes[95]. Some authors[96] argue not only that AmI technologies tend to go beyond the currently existing privacy guarantees, but also that they are changing our expectations of privacy, in terms of its diminution, given that these technologies become a common part of our life. In other words, we are becoming more and more used to see our privacy limited (like, possibly, with increasing use of social networks as 'normal' and essential part of their relationships), and, worst, to be commonly considered as potentially 'suspicious', as demonstrated by the increasing use of detection technologies.

As has been argued, there are no simple solutions to reach the right balance between privacy and security, just as there are no simple solutions to ensure that AmI is beneficial for the citizens, the industry and the governments as well, at the same time. The only alternative seems to be to address those (emerging) threats one by one and to make everyone involved in safeguarding his/her privacy, identity and security[97]. Legal and philosophical debates, in the context of balancing privacy and security, have been lit up both by advocates of the so called "I've got nothing to hide" argument and its opponents: to agree with the latter means recognizing that the issue at stake is not to fully accept or to totally renounce the relative security and surveillance policies, but to verify the related oversight procedures that governments are expected to put in place[98].

It might be useful to evoke here that the European DP directive does not apply to data-processing carried out for the purposes of public security, defense and activities in the area of criminal law (the so called 'third pillar' of the pre-Lisbon Treaty). Many States, nevertheless, have implemented the directive in such a way as to cover also areas related to public security, but with the effect to obtain a European not homogenous framework. After several debates on the opportunity to extend data protection to these areas of action, the European Council has adopted a Framework

[95] I. Maghiros, (ed.) (2003), *Security and Privacy for the citizen in the Post-September 11 Digital Age: a prospective overview*, Report to the European Parliament Committee on Citizens' Freedom and Rights, Justice and Home Affairs (LIBE), Institute for Prospective Technological Studies (IPTS), Seville.
[96] M. Friedewald *et al.* (2007) *cit*.
[97] Wright et al. (2008), *cit*. p. 47.
[98] Solove D. (2007). "I've got nothing to Hide" and other misunderstandings of Privacy, *San Diego Law Review*, 44, p. 745.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Decision in 2008[99], defining the data subject's rights in the context of criminal investigation and other police practices (including profiling): the right to be informed, the right to access, rectify or erase data, activities that should also be made know to third parties to whom the data have been disclosed and a specific obligation to ensure a high quality of data is also provided for, in order to guarantee the correctness of the consequent profiles[100]. Nevertheless, as stressed by the EDPS [101], this decision only covers police and judicial data exchanged among Member States or EU authorities and not to domestic data, leaving the level of protection unsatisfactory. The next chapter discusses how this situation is likely to change with the entry into force of the Lisbon Treaty.

It is interesting to notice how the ECHR, although recognizing the violation of the fundamental right of privacy, had recently arrived at quite different conclusions, in terms of the 'legitimacy' of security and investigative measures (that is, *ex* Art 8 of the ECHR, necessity and proportionality of the public interference in private life for a democratic society)[102]. These discrepancies are also due to the lack of uniformity on the further employment of evidences, gathered through procedures that have infringed the right to privacy[103]. The need for more clarity is even more urgent if we think about the increasing recourse to the electronic evidence as a judicial proof, the lawfulness of its collection being often contested.

To conclude this first chapter, after having analyzed some possible applications of AmI technologies, it is possible to notice that, while the main concern of computer scientists is to make the AmI systems as widely accepted and useful for society as possible[104], the main concern of the jurists is instead to verify, on the one hand, the legitimacy of these technologies according to the existing values deriving from the fundamental rights protection and, on the other, to find out possible legal responses, in order to 'balance' the apparently opposite values (security and predictability, on one side, privacy and identity, on the other). Some steps have been taken in this direction, in order to enhance privacy while developing new automated technologies, but several legal issues remain to be addressed. One answer could be,

[99] Council Framework Decision (2008/977/JHA) of the 27/11/2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
[100] Wright *et al*. (2008), *cit*. p. 47.
[101] EDPS Opinion on the Communication from the Commission to the EP and the Council on an Area of freedom…*cit*. p. 5.
[102] Characteristic are the examples of the decisions *Bykov v. Russia* and S. and *Marper v. UK*, the latter addressing also the adequacy of the safeguards aimed to avoid abuses in the processing of and access to biometric and genetic data. See Chapter II, *infra*.
[103] D. Wright *et al.* (2008), *cit*. p. 86.
[104] D. Cook *et al*. (2009), *cit*. p. 289.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

as discussed above, the adoption of relevant sector-based rules, more adaptive to AmI contexts and privacy needs.

In the next chapter it will be discussed how these challenges for privacy right(s) are issued by a particular kind of new technological scenario, what has been called here the *AmI detection* (or *security*) *scenario*.

CHAPTER II

THE IMPACT OF AMI TECHNOLOGIES ON HUMAN RIGHTS. THE CASE OF *AMBIENT INTELLIGENCE DETECTION SCENARIOS*

1. Preface

The following Chapter will focus on the effects of the increasing use of the so-called 'surveillance technologies' on the privacy right(s): it is referred here to the technological measures adopted by governments (mainly, but not exclusively) for purposes of public security (preventing and countering crimes)[105], among which new *detection technologies* emerge[106].

Each of them presents at least some of the main features of AmI and is, therefore, likely to be used in a complex AmI world. Also due to their relative novelty, they have started to be developed without receiving, so far, the adequate attention from jurists or civil society (at least not everywhere).

[105] B. Bowling, A. Marks, C. Murphy (2008), *Crime Control Technologies*, in R. Brownsword, K.Yeung, *Regulating technology* (eds.) Oxford, Hart Publishers, p. 60. The authors stress out the fact that the power of surveillance using devices such as cameras, microphones, computers, phone taps etc has expanded dramatically in recet decades. They also observes that in the great deal of surveillance activity conducted by the police, local authorities and private companies, the U.K. conducts with its 4 million of CCTV cameras in public spaces.

[106] See *DETECTER Detection technologies, terrorism, ethics and human rights* Collaborative Project under the VII framework program. Documents available at http://www.detecter.bham.ac.uk/.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

As will be discussed, the increasing use of surveillance techniques and of profiling practices is not exclusive to security matters and is common, although in different ways and for different purposes, to both private and public governance, thus, resulting in serious impact on the private life and on related rights of citizens (as individuals and as social members).

At least two main issues can be immediately highlighted with regard to the practices of what has been called '*le gouvernement statistique'* [107]: on the one hand, the threats to the individual right to privacy (as protection of a sphere of autonomy, in his/her private and social contexts) raised by the normative capacity of autonomic devices to predict behaviours and determine preferences and choices; on the other hand, the risks for privacy rights resulting from security measures (that, although 'formally' lawful, could end up in disproportionate practices or unfair decisions. In what follows, it is assumed that, although these issues emerge at different levels, they often intersect.

In what follows, after having presented some of the major techniques caracterizing the security measures of post - 9/11 the focusing will be on the new detection technologies and their challenges for privacy and data protection; the discussion will turn, hence, to the legal instruments currently available and enforceable towards such measures (such as the Art 8 ECHR, in the *Marper* case), as well as on the limits of the current legal framework and on the need for its review, before acknowledging the opportunities and challenges issued by the entry into force of the Lisbon Treaty.

2. How the increasing security measures post 9/11 affect the fundamental right(s) of privacy

As said above, after 9/11, in many regions of the world, including the EU, several changes have been registered in legislation and polic-making, aimed at strengthening security through special investigative powers, mass surveillance programmes and counter-terrorism procedures[108]. As consequence, new and more

[107] A. Rouvroy (2009), *Le corps statistique*, La Pensée et les Hommes, n.74, ed. P. Deled, available at. http://works.bepress.com/antoinette_rouvroy/29/. Of the same author, *Governamentality in an Age of Autonomic Computing: Technology, Virtuality and Utopia*, in M. Hildebrandt, A. Rouvroy (eds.) 2010, *Autonomic Computing and the Transformation of Human Agency. Philosophers of Law meet Philosophers of Technology*, Routledge.

[108] IPTS, JRC, Report on security and privacy for the citizens' freedoms and rights, JHA, July 2003 *Report Series, EUR* 20823. As illustrated in the Report, new legislative measures and political

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

intrusive security measures have been introduced, basing their operability in particular on the use of ICT for data collection, data-mining and data-sharing. Parallel to reinforced powers of governments and law enforcement agencies to access individuals' personal data even for purposes different from those for which they have been collected[109].

It was immediately evident to the most keen and devoted privacy defenders[110] that intensive surveillance systems and preventive control, traditionally reserved for the investigation of criminal suspects or to espionage, were progressively extended to the whole society, to say with G. T. Marx "penetrating in as a laser and absorbing as a sponge"[111] the data of ordinary people, making, ultimately, everybody a potential suspect.

Even outside the sphere of criminal justice, hence, citizens are expected to comply with increasing security measures and investigative applications of technology are increasingly blurring in an atmosphere of 'nothing to hide, nothing to fear'[112].

As stressed by M. Hildebrand, infact, citizens are increasingly "screened, located, detected…supposedly justified by an appeal to security threats, fraud and abuse; at the same time potential customers are profiled to detect their habits and preferences in order to provide for targeted services"[113]. Given the investments made, among others, by the same European Commission, the creation of Ambient

---

initiatives have been adopted to reinforce or adapt the existing systems to the new counter-terrorism exigencies.

[109] See the Report (2009) of the UN Special Rapporteur on the promotion and protection of HR and fundamental freedoms while countering terrorism *A/HRC/13/37*, and P. De Hert (2005), *cit*., p. 69.

[110] Beside privacy advocates working in academic and legislative environments, civil liberty groups and international associations, such as EPIC, Privacy International, EDIGR, Ligues de droits de l'homme, play an important role in critically assess legislative initiatives involving new technologies that can seriously impact fundamental rights as privacy. See *infra*, the EPIC suitcase against the DHS of U.S. on the introduction of body scanners in the airports.

[111] G. T. Marx (2005), Surveillance and society, *Encyclopedia of Social Theory*, available at http://web.mit.edu/gtmarx/www/surandsoc.html, where we can read: "One way to think about the topic is to note that many of the kinds of surveillance once found only in high security military and prison settings are seeping into the society at large. Are we moving toward becoming a *maximum security society* where ever more of our behavior is known and subject to control? Some of the features of this maximum security society are: 1) a dossier society in which computerized record play a major rule; 2) an actuarial society in which decisions are increasily made on the basis of predictions about future behaviour as a result of a membership in aggregate categories 3 a engineering society in which choices are increasingly are limited and determined by the physical and social environment. The author more recently has investigated the surveillance issues also under the child's rights perspective: M.T. Marx, V. Steeves, From the beginning: Children as subjects and agents of surveillance, in Surveillance and Society, vol 7, n. 3/4, 2010.

[112] See Bowing *et al. cit*. p. 62, who affirms: "the Big Brother is not just watching; it is tooled up and on the beat. When examining [the] technological advances, the dearth of legal regulation should cause concern".

[113] M. Hildebrandt (2008a), *Profiling and the rule of law*, Identity in the Information Society Springer, p. 55-70.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Intelligence[114] and 'Internet of the things'[115] will certainly not remain a vision of computer scientists.

Future networked environments, based on real-time monitoring and able to smartly to adapt to our preferences, may end up in being a gilded cage for us[116], if we do not invest also in developing legal and technological tools to contrast the threats of automated profiling (see below).

Control and identification activities are carried out with the use of sophisticated techniques, often of AmI nature, more accurate and potentially invasive than those existing before. An aspect that must be immediately pointed out is that, since often these techniques rely on *smart*, *light*, and *invisible* devices, or even without the awareness of the people who are under their control, they are called 'soft technologies'[117], although their insightful reasoning and acting capability are anything but 'soft'.

The combination of old identification systems (ID cards) with new technologies, relying on biometrics and facial recognition "enable tracking people where they are, where they've been and where they are going"[118]. Moreover, large databases used both in public and private contexts are often created and interconnected and actions to contrast terrorism are taken on the basis of profiles created from these databases through mathematical processes (the *data-mining* processes – see below).

As stressed by the Special Rapporteur in his Report A/HRC/13/37[119], today the erosion to the right to privacy is due to the increasing use of surveillance measures, included new technologies, put in place without adequate legal safeguards.

3. Profiling techniques and general concerns for HR framework

[114] For the concept of AmI see chapter I *infra*.
[115] For the definition of 'Internet of things', see *infra* note 56 ; on the 'Digital Agenda' of the EU see: http://ec.europa.eu/information_society/digital-agenda/index_en.htm: "[…]is Europe's strategy for a flourishing digital economy by 2020. It outlines policies and actions to maximise the benefit of the Digital Revolution for all"; see also the II annual Conference 'Internet of Things' Europe 2010, available at http://ec.europa.eu/information_society/policy/rfid/documents/iotconferencereport2010.pdf and the speech of the commissioner Viviane Reding "A European digital agenda for the new digital consumer" of the 12/11/2009.
[116] *Ibidem*. As the Commissioner stresses, it will be "an environment that anticipates our preferences before we become aware of them"[...]"advanced technologies answer questions we did not raise. They generate knowledge we did not anticipate, but are eager to apply".
[117] For example, iris scan is considered less intrusive than other physical inspections, see De Hert, (2005) *cit*., p. 69.
[118] P. De Hert (2005) *cit*., p. 70.
[119] Report of the Special Rapporteur, *cit*. p. 5.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

As said in the first chapter, one of the key elements for an AmI environment is the profiling, which allows micro computers with high reasoning capability to act or make decisions in an automated (or semi-automated) way, according to the amount of data previously collected[120]. It appears that profiling techniques are increasingly used also in contexts of public security purposes, in particular in counter-terrorism activities[121], deserving, hence, to be mentioned in this paper, before considering more closely the security technologies themselves.

In an AmI world, autonomic profiling allows machines to communicate with other machines and take decisions without human intervention[122]. Given its increasing deployment in different areas (criminal investigation, commercial field), the attention for this practice, and in particular for the profiling based on *data-mining* techniques (dm)[123], has grown up in the last years. The interest is due to the new possible type of *knowledge* that profiling generates and the possible use that can be made of this knowledge, given that "knowledge is power"[124].

[120] The implications for privacy and other fundamental rights of profiling (also in AmI) are addressed by cross-disciplinary scolars in M. Hildebrandt, S. Gutwirth (ed.), Profiling the European citizen, Springer, London, 2008.

[121] See Report of the Special Rapporteur, *cit*. p. 6.

[122] As quoted by M. Hildebrandt (2008b), Defining profiling. A new type of Knowledge in M. Hildebrandt, S. Gutwirth (eds.) *Profiling the European citizen*, Springer, London, p. 27, the concept of autonomic computing has been introduced by IBM in 2001, to give the idea that, like our autonomic nervous system that governs heart and other vital function, also the complex pervasive computing network need to rely on a self-management system. Interestingly, many projects on AmI adopt biology-derived terms ('hoxigen', 'autonomic', intelligence'..) to give the idea that this world adapts and imitate human behaviour and even thoughts. As argued by Hildebrandt, profiling can be understood as a *pattern recognition*, a basic feature of living organisms to survive and constitute their environments: machine profiling can be similar to human profiling to the extent that it is part of autonomic behaviour, but differently from the latter, the machine do not integrate conscious reflection and intentional action.

[123] M. Hildebrandt, (2008b) *cit*., p. 18, who defines *data mining* as "the procedure by which large databases are mined by means of algorithms for patterns of correlations between data. These correlations indicate a relation between data, without establishing causes or reasons. What they provide is a kind of prediction, based on past behaviour; in this sense profiling is an inductive way to generate knowledge". The technical process including data selection, data analysis and interpretation of the outcomes is called Knowledge Discovery from Databases (KDD), A. Canhoto and J.Backhouse, General description of the process of behavioural profiling, in M. Hildebrandt & S. Gutwirth (2008), *cit*., 47. For a description of data mining techiques applied to law, A. Stranieri and J. Zeleznikow, Knowledge *Discovery from Legal Databases*, Springer, 2005.

[124] M. Hildebrandt (2008), *Profiling and the rule of Law*, *cit*., who stresses that in order to understand the potential threats deriving from these techniques, we need to look into the asymmetries between citizens on the one hand and the large organizations that have access to their profiles on the other hand: not asymmetry of access to personal data but asymmetry of access to knowledge. A more suitable metaphor other than the Big Brother (often used in dataveillance discourse) would be, hence, that proposed by D. Solove (*The Digital Person. Technology and privacy in the Information Age*, NY University Press, New York, 2004) of Kafka's process, describing the indifference of the computers while collect our data, but capable of providing the evidence for a conviction at certain moment. See also P. Guarda, the Myth of Odin's Eye: privacy vs Knowledge, in M. Ferndandez-Barrera *et al., Law*

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

The increasing amount of data created in many contexts of the current Information Society can be filtered, allowing the selecting of information from 'data noise'[125], and processed by means of profiling techniques to create 'knowledge' - it is said that we live in a 'Knowledge society'.

Profiling is the output of data-mining algorithms: as mathematical procedures, these algorithms can be used to identify (possible) relationships and trends in several databases; in other words, they can discover ('detect') significant and (statistically) frequent patterns in large amount of data, which can ground a decision-making process[126]. Some authors underline the societal impacts in case of discrepancies in databases, such as the increase of false positives or overlapping of profiles that make them less effective instruments of identification (especially in case of widespread application) and as a basis for unfair decisions [127].

Group profiling techniques (used to select individuals as members of a group and to exclude those who do not fit the profile and that may lead to an unfair treatment) raise general concerns for human rights legal framework: in case of automated profiles bringing to discriminatory classification of people (and the related denial of services or access), the anti-discrimination law (e.g., the art 14 ECHR) could be not enough to face the effects of these new technologies, especially in the case of indirect discrimination[128].

Important types of profiles, for their construction and typical application in an AmI world, are the 'non-distributive group profiles'[129]. A person who is ascribed to one of these profiles is said to be, statistically, a person who will have certain behaviour (whatever we deal with, be it marketing preferences or criminal attitude):

---

and Technologies: Looking into the future. European Press Academic Publishing, Florence, 2009, p. 243.

[125] See among other definitions, http://www.lynchpin.com/white-papers/understanding-data-noise.

[126] See Anrig, Browne *et al. The role of algorithms in profiling*, in M.Hildebrandt & S. Gutwirth (eds), *cit*., 65, who suggests the adoption, especially in the complex environment of AmI, of probabilistic algorithms (i.e., incorporating additional human knowledge), better than deterministic ones.

[127] J. Van Bendegem (2008) Neat Algorithms in messy environments, in M. Hildebrandt & S. Gutwirth (eds) *cit*, p. 80.

[128] That is a kind of discrimination not based on one of the criteria such as those *ex* art 14 HCHR, but on apparently neutral criteria, e.g. place of residence, credit account, or meal preferences. See W. Schreurs *et al.* (2008), *Cogitas, Ergo Sum. The role of data protection Law and non-discrimination law in group profiling in the private sector*, in M. Hildebrandt & S. Gurtwirth (eds.) *cit*. p. 264; the authors underline that in this cases, if there is no objective and reasonable justification or if there is no reasonable proportionality between the means and the aim pursued, the treatment is discriminatory. One main related issue is defining who is responsible in case the knowledge produced by profiles facilitates illegitimate indiscrimination or other unforeseen effects.

[129] Most groups of people have a non-distributive profile, that means that not all members share all the attributes of the group profile (like instead is for a distributive profile of, for example, all the students of 20 years old).

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

in this sense are called *predictive profiles*[130]. The problem is that the resulting profiles that are applied to a person (because her data match the profile) are often generated by data-mining other people's data: profiles are applied to people whose data were not used to create these profiles[131]. That means that the application of the group profile to an individual member of the group can bring about to a wrongful attribution of preferences or risks[132].

An important issue to underline is that members of this type of group do not share the relevant attributes but they will be treated (i.e., be offered of certain services and products or be pursued as criminal) as they do (living in a certain neighbourhood that is profiled as risky one); the technique can therefore cause - and indeed has caused- unfair discrimination.

As noted by some scholars, in front of these profiling practices data protection regulation shows its limits, since it applies to identifiable person[133]: it is not so useful when profiles are inferred from amount of data, often anonymous, of many other people[134].

---

[130] As underlined by D. O. Jaquet-Chiffelle (2008), *Direct and indirect profiling in the light of virtual persons*, in M.Hildebrandt & S. Gurtwirth (eds.) *cit*. p. 41, using data mining techniques, subsets of persons sharing some attributes can be defined, creating in this way generalized categories of people. In other words, the category (or virtual person that allows the representation of the corresponding category) results from a process of generalization. With each category, then, is associated the inherited profile. According to Jaquet-Chiffelle, *indirect* profiling (i.e. the profile applied has been derived from other subjects, like Amazon's personalized offers, based on other users) is less reliable then a direct one, since it bases on generalization, with the consequence to be applied to subjects that do not share the same attributes.
There are, nevetheless, authors (see B.-J. Koops (2008), Some riflection on profiling, in Hildebrandt & S. Gutwirth (eds.) *cit.* p. 327) that give a less alarmist perspective of profiling techniques, not always involving negative effects for citizens and that doubt about the possibilities offered by 'counter-profile the profiles'- transparency tools- to restore the balance of power: the suggestion is a paradigm shift (law builted in technology) and focusing more on wrongs than on preventive abuse, on discrimination more than the privacy.
Critics of PET (such as P3P or anonimizer.com) and their aim of data minimization are expressed by Els Soenens, in H. 170, who suggests a transparency approach: instead of merely reducing the exchange of personal data she claims the principle of minimum data asymmetry, focusing on establishing a balance between the information detained of the users and that by the data processors/profilers (that means for the user to be allowed to access the profiles applied to her, change her preferences).
[131] M.Hildebradt (2008) *Profiling and the rule of Law*, *cit*. who stresses the difficulty in apply the data protection regulation, focused on *personal* data.
[132] D. O. Jaquet-Chiffelle*, cit.* p. 41.
[133] W. Schreurs, *et al. cit.* p. 241. According to the authors, the directive risks to be unuseful (if not integrated in technology) against unfair or illegitimate exclusion on the basis of group profiling, especially in case of profiles generated from other people's data or derived from anonymised data: this being valid both in private and public sectors, where the data protection logic is countered by data retention and public order logic.
[134] Doubts are also expressed by R. Leenes (2008) Addressing the obscurity of data clouds, in M. Hindebrandt & S. Gurtwirth (eds.), *cit*. p. 293, about the adequateness of data protection tools: according to the author, the protection of the transparency right may be available only after the application of the profile to an individual; moreover it presumes that the subject is aware that decisions are taken on the basis of these profiles and this is often not the case. Thus, according to the

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Others ascribe the inadequacy of data protection law in certain areas of the society, such as employment, to the focus of the European directive on the individual instead of the collective dimension, suggesting, hence, more radical solutions[135]. This offers a support for the assessment of data protection and privacy rights as social and collective goods, that should be addressed and protected as such with the appropriate instruments, taking into account the implications for democracy and its values.

The main threats deriving from profiling can be recalled here.

- Persons are being profiled, without access to the knowledge that is used to categorize them: this results in damage to people's personal autonomy and freedom, since they cannot anticipate the actions of those who know about them (see later Rouvroy).

- Moreover, the right of the subject to obtain information about the logic of any automatic processing of data concerning him can crash with the propriety rights of the owner of the profiling system, with the consequence that the subject is denied to access to the technologies used and to provide a proof in a proceeding (due process limitation)[136].

- An AmI world, in particular, relies on sensors and biometric applications connected with online databases and softwares that allow a continuous process of real-time profiling. In other words, the intelligence is not situated in one device but emerges in the interconnections with the others: with 'the Internet of the things', the online

---

author, we do not really have effective legal or technological tools for protection against the unfair stereotyping made possible through profiling.

[135] In this sense, see P. de Hert (2008a), The use of labour law to regulate employer profiling: making data protection relevant again, in M. Hildebrandt & S. Gurtwirth (eds.), *cit*. p. 226, who invites for the adoption of criminal law prohibitions for an effective protection against the current surveillance trends. As de Hert notes (*ibid*. p. 231), the call for recognition of a collective dimension of privacy is not new in international human rights law: new refugee patterns have brought legal scolars to recognize the need for refugee rights that are not only granted to the individual refugee but also to refugee groups in need of protection. It could be noted that data protection regulation partly recognizes a collective dimension of privacy, as testified by its administrative tools (See the same author, p .232. and D. Le Metayer & S. Monteleone, Automated consent through privacy agents, *cit*. p. 139), but the predominant system of regulation applied today is based on the idea that the processing is made legitimate simply by the consent, considering everything as a potential object of trade. A part from the cases in which the consent is even not in question – like in the case where data processing is necessary for security purposes - and although self-regulation could be a useful instrument in many case, public intervention should be necessary and the law should have still a fundamental role, also and *a fortiori* in a 'knowledge society' as the contemporary one, where there are even more considerable differences among persons and groups in accessing to knoweldge and to the power (power asymmetries), and where the consent often cannot be said as freely given.

[136] M. Hildebrandt (2008b), *cit*. p. 261. In many cases this knowledge is even protected as part of trade secret or intellectual property, to which the citizens have no access at all. Sell also N. Van Dijk, Property, Privacy and Personhood in a world of Ambient Intelligence, *Ethics and Information techologies*, Springer, Issue 1, vol. 12, p. 57, available at http://www.springerlink.com/content/951568p67r18h5q5/.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

world - with its capability to collect, store, aggregate and mine behavioural data - integrates the offline world, amplifying the risks of each techniques.

- Unprecedented risks can derive from highly personalized profiling, especially in case the users have no feedback on what happens to the data they 'leak' while moving around in their animated environments"[137].

As far as autonomy is concerned, as said before, personalized profiling, that are becoming essential in organizational strategy in business and government sectors, has also potential impacts on societal values like autonomy and diversity; as pointed out by van der Hof and Prins[138], serious drawbacks that can derive from the integration of personalized services into the vision of AmI are the augmented risks of inclusion and exclusion (on a refined scale), against which it becomes essential to ensure the *transparency* of the way profiling is constructed.

If profiling mechanisms are deemed as irrefutable in our times the challenge will be how to prevent their are in 'dataveillance'[139], normalization of individuals that counter the effectiveness of rights acknowledged by the law, such as freedom, privacy, due process.

Some scholars convincingly identify as preconditions for the exercise of these freedoms and rights in profiling age some 'meta-rights', such as the right to oblivion, right to disobedience and right to be aware and make others aware[140].

3.1. Data-mining techniques (or… what if algorithms decide for us?)

Two more notes are necessary on data-mining techniques (as defined *supra* in note 124), essential for the profiling activities in a world of ambient Intelligence[141].
As noted by O. H. Gandy& H. Schiller, in the last decades there has been an increasing demand of data-mining tools, both due to the offer of commercially available services and software products in the marketplace and the government incentives for expanding research on related applications.

In the U.S., even before 9/11 private companies and governmental departments have been involved in merging public and private databases for example

[137] M. Hildebrandt (2008b), *cit*., p. 23
[138] Van der Hof and Prins (2008), *Personalization and its influence on identities, behaviour and social values*, in M. Hildebrandt & S. Gutwirht (eds.) *cit*., p. 111.
[139] See I Chapter *infra*.
[140] A. Rouvroy (2009), *cit*. p.191, speakes about "droit à l'oubli, droit à la désobéissance, droit de se rendre compte et de rendre compte".
[141] K. De Vries (2010), Identity, profiling algorithms and a world of ambient intelligence, *Ethics and information Technology*, 12 (1), p.71-85.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

for the analysis of workforce trends. After 9/11 one of the answers to the pressing security concerns emerged was to expand the use of data-mining: Internet communication firms offered their expertise in dm - in particular modelling of behavioural and patterns predictive analysis products, usually aimed at targeting advertising - to develop these technologies in order to identify suspicious activities and potential terrorists, although the main technology experts were doubtful about their predictive capacity[142].

Since the first announcements of these investments in technologies there was a concern that the development of these systems and their routinely use by defence and security agencies could increase the chance that they become available as off-the-shelf commodities for use in commercial sector[143].

One of the main features of data-mining is that these systems facilitate the extraction of data and classification of individuals in groups, allowing their segmentation and discrimination (discriminatory technology used by commercial firms for the pursuit of profits).

Gandy & H. Schiller affirm that even efficient techniques should be banned or limited because of the unacceptable social consequences, in consideration of the basic principles of society, (see below about privacy as social good).

Although some could claim the economic efficiency of using discriminatory personal attributes - race, gender, age, class- correlated with behavioural indicators, serious concerns about human rights arise: "if we allow decision makers to use race, gender and other markers of group identity as a basis for exclusion from opportunities, then we will only strengthen the correlation between group membership and social status"[144].

---

[142] O. H. Gandy& H. Schiller (2002), *Data Mining and surveillance in the post-9.11 environment*, IAMCR, Barcelona.

[143] *Ibid*. p. 11. The diffusion of the technology to the commercial sector appears to be accelerated also by the activities inspired by 'homeland security', as promoted by the U.S.A. Patriot Act, that generated new concerns in privacy advocates for the availability of details about individual's searching on Internet (and the easy access to the content of files accessed by the users).

[144] *Ibid*. p. 12. The authors give the examples of the so called *web-lining* techniques – data mining in electronic commerce that operate a geo-demographic discrimination- as the relining techniques used by banks and forbidden - which exclude people from access to services and products on the basis of race or other kind of discrimination. The point is that the victims of web-lining are less aware of their status and, hence, they have less possibility to challenge their exclusion from possible opportunities. They also stress that a privacy framework which, as in the U.S., emphasizes 'individually identified information' are mostly meaningless as a defence against the social harms that data-mining represents and notice that the power of dm is not in its ability to create specific profiles but to increase the benefits to be derived from controlling the behaviour of members of well-defined groups. Apparently, in the U.S., examples of racial discrimination and denial of bank services on the basis of the zip code of residence are not rare.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

It is, mainly, due to this controlling power that data-mining techniques are relevant also in an AmI discourse[145] and should be particularly pondered when assessing AmI applications, either in commercial or in security contexts.

It must be noted that in the commercial sector, where data mined from different sources may be used and in which the key requirement allowing (or denying) the use of these data should be the consent of the subject, the "individuals are generally provided with a meaningless choice between doing without and providing a blanket license for whatever uses of information a data manager decides is appropriate" [146].

The efforts made in the last years in particular by the European policies to limit the storage of data for no longer than necessary and for purposes related to initial collection are reversed by the new regulation on data retention and by the strategies (common to EU and other countries) of greater sharing of data by public and private organizations as well as by governments.

A part from involving the public opinion, in order to raise awareness of the social costs of discriminatory technologies (such as data-mining and use of derived profiles based attributes such as race or ethnicity), a renovated framework of general safeguards to marginalize the negative impact of these 'controlling technologies' seems necessary.

3.2. Biometric profiling and other features of AmI: old and new threats for HR

Attentive studies warn against the risks of a revolutionary use of biometrics which can go further than their core capabilities (i.e. identification and verification), and in particular of *advanced group profiles* that, linking biometrics with other data, create sophisticated profiles of persons in different contexts: although the apparent precision of their sophistication, risks are still possible for the rate of false positive and false negatives produced [147] and for the capability of extensive monitoring.

A type of group profiles relevant for AmI visions is the *behavioural* profiling (i.e., the study of patterns of behaviour, performed through data mining) and*, in*

[145] See K. De Vries, *cit*. p. 71.

[146] O. H. Gandy& H. Schiller (2002), *cit.*, p. 15. The authors seem quite sceptic about the role of information rules that should guarantee to the subjects the access to data about them, as they doubt that the user can challenge the cumulative score that has been assigned to them by data-mining operation: very few would understand the complex algorithm that produced it. See the similar considerations of M. Hildebrandt (*infra*).

[147] See DETECTER Survey 5, *cit*. p. 21.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

specie, the *behavioural biometric* profiling[148]. The profiles in this case are deduced from data collected by the sophisticated sensors disseminated in the AmI environment, that record, store, aggregate machine-readable data of 'behaviours' such as speech, facial expression, gait, gesture and in the near future also smell[149]. High expectations of these technologies, that is considered essential for a real time monitoring and customization of AmI- and parallel risks for fundamental rights - seem to be based on the possibilities offered by the semantic web (that should allow a more intelligent pattern recognition)[150] and on the integration of pattern recognition devices that mine data from different modalities (e.g., speech recognition on the basis of both voice and lip-movement recording): "the total information that can be extracted from behavioural biometric measurements forms an especially rich profile for the subject of analysis"[151].

Although fascinating technologies, their advocates seem to be guilty of technological determinism, believing that certain data really express certain behaviour, disregarding for the context in which they are collected[152]. This attitude (dangerous for HR discourse) brings them also to affirm too promptly that, since behaviour is easy to observe, many of these techniques are non-intrusive, and the subject may not even be aware of them (see later on soft technologies)[153].

In view of all the mentioned risks, and although the importance of some existing technological solutions has been acknowledged, a lack of legislative protection

[148] A. Yannopoulos, *et al*. Behavioural biometric profiling and Ambient Intelligence, in Hildebrandt & S. Gutwirth, *cit*, p. 89.

[149] See the International conference *Computer Privacy & Data Protection*, Bruxelles, 29.01.2010, http://www.cpdpconferences.org/CPDP2010.html.

[150] This would ease the 'Internet of the things' (*supra*), in which the data collected through sensors operating potentially in evey building, vehicle, outdoor space are 'hosted' online: "Soon, the kind of sensors that people are already buying- microphones in mobile phones, digital cameras, web cameras, motion detecting devices, medical sensors measuring e.g. heartbeat…environment monitoring sensors- will be online and thus globally accessible, barring only policy contraints", A. Yannopoulos *et al*. *cit*., p. 102. It will be, therefore, determinative to know who is going to decide on these policies and whether they are adopted. On the concept of semantic web and its development see P. Casanovas, *The future of Law: Relational Justice, Web Services and Second-generation Semantic Web*, in M. Fernandez-Barrera *et al. cit*., p. 137, who pointes out that recent developments in semantic technologies, natural languages processing, web 2.0 and web 3.0 may contribute to the convergence of different approaches to see the interplay of law and technologies into a single techno-legal one.

[151] Yannopoulos, *et al. cit*. p. 103.

[152] J. Backhouse, Old metaphorical wine – new behavioural bottles, in M. Hildebrandt & S. Gutwirth, *cit*. p.104, who invites for a better study of the social context in which prifiling technologies function.

[153] Interesting in particular the definition of emotional recognition, as the task of processing a stream of data with the understanding that it reveals the emotional state of its subject: "[..]if we wanted to detect either extreme agitation or extreme boredom in the speech of a subject, we could record the speech signal, compute a measure of its speed, compare this to an acceptable measure of 'average' or normal' speech speed and specified that fast speech is to be considered as agitated and slow speech as boredom" See again A. Yannopoulos *et al*. p. 91.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

against the loss of control on biometric profiles and discrimination has been denounced, in particular by Art 29 Working Party[154].

The main problems seem in particular to derive from the use of biometric characteristics as a link to other profiling information. As noted by Kindt [155], in case the biometric data is capable of linking the profiling information with a specific person (*hard* biometric, i.e. it is capable to identify a specific person, as in the case of facial image) the risks of central storage of biometric data denounced by Art 29 WP are applicable. However, legal attention is needed also for central storage of *soft* biometric characteristics (incapable of direct identification or verification) used in profiling applications (an individual's height or weight), because they contain similar risks: first, in combination with profiling applications, they may result in sensitive information (health); second, soft biometrics and profiling may also have the capability to qualify individuals in groups for their characteristics (tall, angry people, etc.). The author stressed that, this qualification of individuals according to human characteristics by profiling applications (and the following use of related profile) may need to be better protected then others (e.g. consumer data that may easily change).

The afore-mentioned dangers seem to grow up with the governments' surveillance practice, emerging after 9/11[156], to draw on also private and commercial databases[157] and with the fact that more and more services are accessible by biometric data-processing[158].

---

[154] See Art 29, DP Working Party, *Working document on biometrics*, WP 80 of the 01.08.2003.

[155] E. Kindt, (2008) Need of legal analysis of biometric profiling in M.Hildebrandr & S. Gutwirth (eds.), *cit*., p.142.

[156] V. Andronikou et al. *cit*. p. 135 write: "Biometrics, serving as links to an individual's profile, offer the opportunity to create a trace of an individual's actions, daily activities. This might be justified for tracking an individual who is considered a suspect or a potential criminal. Thus if/when this person engages in an illegal action, a backtracking process would provide important information that may reveal previously committed but not detected illegal acts. Security reinforcement through the integration of biometrics into security systems is an important application […] in an effort to protect the present by using information from the past"; they explain, thus, that while watch-lists are composed including wanted persons or other police records they "cannot really offer any answer when it comes to the virgin illegal act of a person, suicide terrorist and generally people from whom no enrolled data exist. Biometrics profiling in this case promise to fill in the gap…so that the detection of potential criminals will also be possible".

[157] See Art 29 DP Working Party, *Opinion 2/2004 on the Adequate Protection of Personal data contained in the PNR of Air Passengers to be transferred to the U. S. Bureau of customs and border protection*, WP 87 of the 29.01.2004.

[158] See E. Kindt, *cit*. p.141, who reminds that biometrics will soon be used in large-scale applications, e.g. for biometric passports.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Behaviour such as "walk like some terrorist does, or sport a beard like a freedom-fighter…might be classified and used as triggers for important governmental intervention and reaction. The intelligence of the machine will then be critical"[159].

It is possible to draw analogies between privacy concerns which have recently arisen (for Rfid, biometrics, etc.) and those likely to arise in an AmI world, but probably not sufficient to consider all the new impacts that these technologies will be able to produce.

Detailed recommendations have been adopted in Europe by Art 29 Working Party, for instance, on the use of RFID, that could have an impact on privacy right and international best practices for the implementations of RFID have been published by the Centre for Democracy and Technology[160], recommending that notice should be given when data are collected from a Rfid system and eventually transmitted to third parties, as well as that, when possible, individuals have a choice about how the collected data is used and to access to the same data.

Similarly, concerns regarding the wireless network, another technology that is becoming part of pervasive computing environments are emerging: as the network is going to cover more and more area, companies or governments, managing the wireless systems, it could capture the content transmitted over them, and in light of the possibilities given by GPS system to localize people and the constant authentication required, the network operators have the ability constantly to survey individuals[161].

In a pervasive computing world, networks will be extended (we hear talking about 'Internet of the things'), and the devices that people will carry with them (or even wear) will be constantly able to transmit data about what the person is doing and where he/she is doing it, allowing network operators to spy every move.

---

[159] J. Backhouse, *cit*., p.106. As R. Leenes, Mind the step, in M.Hildebrandr & S. Gutwirth, *cit*., p.160, estimates, if some profiling technologies (such as those based on location data) are likely too complex and expensive to be used for commercial services, the state may invest in such kind of profiles (that 'provide a permanent stream of data, allowing the construction of very informative profiles if combined with other data') urging their adoption in the fight against terrorism and crime.

[160] See J. Ridges (2008), What happens when everything becomes connected: the impact on privacy when technology becomes pervasive, *49 South Texas Law Review*, p.734, who considers them the possible basis for the creation of best practices guidelines for pervasive computing in U.S. and abroad. See also the Communication of the European Commission (COM (2007) 96), Rfid, Steps towards a policy framework, http://ec.europa.eu/information_society/policy/rfid/documents/infso_com_2007_96.pdf, RFID, in which it is claimed that **"**privacy and security should be built into the RFID information systems before their widespread deployment ("security and privacy-by-design"), rather than having to deal with it afterwards".

[161] See J. Ridges, *cit*. p. 735.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Since pervasive computing will simply entail development of the basic technologies already existing, many privacy issues regarding emerging technologies have already been settled[162], but a deeper reflection is needed since the complex AmI scenarios are likely to generate new concerns. These concerns are due to not only the fact that overlapping technologies could threat multiple rights in the same time, but also to the fact that it could happen in a more pervasive way[163].

Two observations can be made: firstly, if the Knowledge Society needs wider collection of data and profiling technologies to 'manage', make sense of the big amount of data and have the control of the results of certain actions[164] – through the prediction of the behaviours, those who can access to these profiling techniques have enormous power of control and anticipation/prevention[165]; secondly, the existing law alone is not sufficient to ensure enough control on personal data and needs to be integrated by technologies embedding the basic values underlying the rights.

3.3. Strengths and weaknesses of data protection legal framework

In front of the profiling activities and the smartness of new devices, data protection regime shows infact its limits, since it has been observed it fails to protect individuals, because it focuses on protecting '*personal data'*, instead of protecting a person against unwarranted and unaware application of profiles, therefore not allowing to exercise the right to access to profiles.

A fortiori, it is possible to argue that the massive collection and storage of data for profiling aims impede the enforcement of the data protection regime to the AmI automated devices[166], that operate often without the need specifically to identify a person: although many of them are far to be recognized as personal data, their impact on individuals could be even more considerable. This, not only because even

[162] J. Ridges, *cit*. p. 737. It is possible to have some idea of sensor networks from the *Sense* project: http://www.sense-os.nl/.
[163] D. Wright et al. (2008), *cit*. p.46.
[164] A. Rouvroy (2009), *cit*. p.191.
[165] For a different perspective on profiling see T. Nabeth, Reply to M. Hildebrandt, in M. Hildebrandt & S. Gutwirth (2008) *cit*. p. 31, who invites to explore the positive effects that personalization practices could have on individual learning or working processes, on one side, and on avoiding our reliance on unjustified categorizations, bias that people perform in everyday life. *Contra*, A. Canhoto and J.Backhouse, *cit*. p. 57, who highlight the role of the data analyst in the process, the social norms and the personal bias of which are likely to inform the outcomes of the mechanical process: "far from being the discovery of an objective truth, profiling is an activity where subjectivity matters".
[166] A. Rouvroy (2008), Privacy, data protection and the unprecedent challenges raised by Ambient Intelligence, *Studies in Ethics, Law and Technology*, Berkley Electronic Press, 2, 1.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

anonymous data (e.g. a code, a date of birth), if correlated, could bring to personal identification, but because the 'personalization' of the environments is sufficient for the *dataveillance* practices - i.e., data mining, profiling and smart control devices - of what has been efficiently called the "*gouvernement statistique*"[167].

Although the validity of its main safeguards[168], there is, at least in Europe, a clear need for a renewal of the data protection regime[169]. In view of these limits [170], privacy right tools can come *où socours*, in a systematic approach that combines these tools.

As noted in the first chapter, some scholars make illuminating distinctions among opacity tools (privacy, as prohibitive protection) and transparency tools (among which data protection, as regulation of the processing)[171]: regarding the profiling activities[172], the extensive processing of personal data is justified only if

[167] A. Rouvroy (2009), *cit*., who observes: "Ce ne sont pas les sujets qui se trouvent objectivés par les dispositifs de surveillance, mais seulement – et c'est notamment ce qui fait paraitre le gouvernement statistique tellement inoffensif- leurs miroitements distincts et fragmentés, digitalisés".

[168] As showed, with regard to identity theft, by the Report to the European Parliament Committee on citizen's freedom and rights, JHA, developed by B. Clements, I. Maghiros, L. Beslay, et al. (eds) *Security and privacy for the Citizen in the post- September 11 Digital Age. A prospective overview*, European Commission, IPTS-Report Series, EUR 20823, July 2003.

[169] See S. Gutwirth *et al.* (eds.) 2009, *Reinventing Data Protection?* Springer, London. A call for a legislative reform "especially now that the data protection is enshrined by the Charter of fundamental rights of EU", with a focus on the role of National DP Authorities, also comes by the EU Fundamental Rights Agency (FRA), See the document *Data Protection in EU: the role of National Data Protection Authorities – Streinghtening the fundamental rights architecture in the EU II*, available at http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf.

[170] It must be noted again with P. De Hert and S. Gutwirth (2009), Data Protection in the case law of Strasbourg and Luxembourg: Constitutionalization in Action, in S. Gutwirth *et al.* (eds.), *cit*. that these limits are more procedural than substantial, as the main principles enshrined in the data protection law are tied to fundamental values, from the realization of which the society would benefit.

[171] See De Hert, S. Gutwirth (2006) Privacy, Data Protection and law enforcement. Opacity of the individual and transparency of power, in E. Claes, *et al. cit*.: the difference, according to the authors is testified by the different Art 7 (reproducing art 8 ECHR) and Art 8 of the EU Charter of Fundamental Rights. See also R. Brownsword, Knowing me, Knowing you-Profiling, Privacy and the Public interest, in M. Hildebrandt & S. Gutwirth (2008) *cit*. p. 345, according to which, the threats of profiling are both opacity and transparency, since we lose opacity as technology eroded our privacy interest and we lose transparency as regulators' strategies undermines dignity of moral choice. "the process is insidious; Big Brother does not announce itself with a Big Bang: it is simply a process of technological accumulation". Therefore, we need "stronger foundations for privacy and dignity than the shifting sands of local practice". In other words, there is a need for greater clearity and accuracy within the law.

[172] As S. Gutwirth & P. De Hert, Regulating profiling in a democratic constitutional state, in M. Hildebrandt & S. Gutwirth (2008) *cit*. p. 281, notice, people are becoming sources for a very extensive profiling devices creating knowledge that affects them: such a profiling, with its threats of individual behaviour custumosation and normalisation, loss of control, enlarged inequalities, erosion of freedom, unmotivated decisions about individuals, require a more attentive monitoring from the perspective of democratic state. The best way to counter these threats would be an appropriate articulation of both opacity tools (more typical of U.S. tradition) and transparency tools (a European strength).

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

transparency tools are made available, empowering citizens by making transparent the processing[173].

As the current data protection regime is inadequate to control and limit the surveillance practices, its point of strength (transparency) should be completed with better defined rules in order to obtain a stronger and "general framework to limit the surveillance"[174] (that could have both private or governmental nature).

It must be acknowledged with M. Hildebrandt that "to reduce privacy to private life would disregard the public nature of privacy and turn it into a commodity to be traded within the private sphere".[175] She notices that privacy is protected by means of a set of human rights (from due process to free speech) but it could be argued also the contrary: privacy could offer its significant support to other rights.

With the advance of sophisticated profiling technologies, privacy could also become instruments for the protection of other fundamental rights, such as freedom, due process, non-discrimination (as discussed below).

3.4. Towards an Ambient Intelligent law

All these reflections seem, in particular, to support the Hildebrandt's vision of *Ambient law*[176] , a new way to intend legal and technological normativity in the profiling age and in an AmI world. The author starts her brilliant essay, with a transposition of the Dewey's concern (democracy implies that those that suffer the indirect consequences of a decision or action have found a way to participate in the decision) in today's world: citizens who suffer or enjoy the effects of Ambient Intelligence should be able to influence the decisions regarding the funding, designing and marketing of these technologies. Being aware that technologies are neither good nor bad, they can be constructed in different ways with different normative implications[177].

[173] In Gutwirth and de Hert's view, privacy provides an essential rule in a constitutional democratic state representing a legal weapon against the development of an absolute balance of powers (that explains why art 8.1. ECHR is, by default, prohibitive and normative: "privacy imposes a balancing of power and resistance in all power relationships", that should apply to the interference of the state but also of companies, police, *etc*.

[174] P. De Hert (2008b), Identity management of e-ID, privacy and security in Europe. A human rights view*, Information Security technical Report*, 13, p. 73.

[175] M. Hildebrandt (2008b), *cit*. p. 311.

[176] M. Hildebrandt (2010), *A vision of Ambient Law*, in R. Bronwsword & K Yeung, *Regulating technologies*.

[177] M. Hildebrand (2010), *cit*. p. 174.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Significantly, she compares the paralysing technological determinism of today with the fatalist acceptance of a natural disaster. Development of technological infrastructures (as AmI), with their impact on the citizens' life, cannot be left mainly to technicians, scientific research or market forces, meaning with that, that governments should actively intervene; *how* and on *which* technologies are major issues for lawyers and engineers of current age.

The need for the creation of Ambient Law is motivated, according to Hildebrandt, by the relevant normative impact that the realization of the AmI vision would have on our everyday life. This impact would be able to change the set of positive and negative freedoms (that are at the basis of a constitutional democracy) if we don't find "the way to articulate the legal framework of democracy and the rule of law into the technological architecture it aims to articulate": this technological embodiment of legal norms is precisely *Ambient law*, that will require a mutual transformation among lawyers and computer scientists[178].

Both law and technology can be *regulative* or *constitutive*, but the constitutive (i.e., *determinant*) capacity of modern law is limited by the fact that it is mediated by the 'technology' of the printed script, which cannot enforce many of the rules it affirms[179].

As Hildebrandt observes, the fact - relevant for further consideration on rule of law in a democratic society - to recognize that technologies have a normative impact doesn't entail the equivalence of legal and technological regulations nor that law or technology are *per se* determinant (constitutive) of human behaviour, since social interactions and market forces have normative impact too. The difference is made by the fact that "Law rules at a meta-level", meaning that it provides the framework within which market, citizens and government can interact (178).

Consequently, the legal and technological measures are not exchangeable tools to achieve policy objectices, disregarding the values incorporated into these tools.

Technological devices should be regulated by the law, "precisely because they are able to regulate and constitute our interactions". In other words, as far as

[178] The normative impact of technologies is meant as their capacity to *regulate* (inducting or inhibiting) or to *determine* (enforcing or prohibiting) certain behaviour: the author indicates, as an example of the first type, a smart car that may warn the driver of her detected tiredness, inducing the driver to stop; of the second type is a car that, after directing the driver to a parking space, technically prohibits her to continue the trip. See M.Hildebrandt (2010), *cit*. p. 189.

[179] In the example of the speed limit, the printed script cannot enforce it, while other technolgocial devices could: a speed limit system built into a smart car is, according to Hildebrandt, an example of legal rule embodied in the machine.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

technological devices have a normative impact they should be brought under the regime of democracy and rule of law[180]. That having been said, and looking how they can better relate, Hildebrandt considers necessary the transition of the written law (inseparable from its embodiment in the script) into a law embodied in other (e.g. contemporary) technologies[181].

The need to reinvent the legal normativity for a digitalized, intelligent world is in Hildebrandt's opinion directly linked to our future ability to access the *knowledge* created by the technologies[182]. An active involvement of both computer specialists and lawyers is necessary to find out which technology will sustain constitutional democracy and how technology can be designed to allow the right balance between opacity and transparency tools [183]. In other words, it seems that we should think about integrate core values into core functionality[184].

Furthermore, it must be stressed with Hildebrandt that the anticipation of the normative impacts by, for instance, technology assessment should inform policy choices at a political level (see below about the *Privacy Impact Assessment*).

An aspect particularly relevant for a discourse on security enforcement in Ambient Intelligence is that the regulative force of technology will be brought within the domain of law, as far as effective possibility to contest the legitimacy of applications of legal rules by means other then the scripts are provided. As stressed

[180] It is possible to see a certain echo of this vision with the recent approach followed by the German Constitutional court (published on 27/02/2008, 1 BvR 370/07; 1BvR 595/07), which seems to recognise the value of a basic right to have digital identity protected and secured, see P. de Hert, (2008b) *cit*. p. 75: although the Court was ruling on the secret online searches by government agencies, the relevant principles and the recognition of the right to confidentiality and integrity of information systems, are still valid also in an 'Internet of things': ICT systems, especially in their interconnection (as it will be in AmI) make possible, according to the Court, "to get insight into relevant part of the conduct of the life of a person or even gather meaningful picture of the personality"; exceptions are thought by the Court to be limited to real danger; the Court seems moreover to refer to privacy enhancing technologies - PET-, when requires that the state spying measures should be limited by *ad hoc* technical solutions in order to respect the "core area of the conduct of private life".

[181] Risks of failure to rearticulate legal norms in the technological infrastructure are possible (see chapter I, *infra*), being therefore essential to establish *how* legal norms should be embodied in *which* technological devices. A digitalized law will continue, anyway, to depend on written and unwritten law, extending its aim and capacity to provide protection (M. Hildebrandt (2008b), *cit*. p. 186).

[182] M. Hildebrandt (2008b), *cit*. p. 185. Equal application of legal norms to equal cases are confronted with personalization made possible by data-mining technologies; the delay of the current procedural safeguards are confronted with the real-time decisions taken by multi-agent systems in smart environments. Since knowledge creates power, a reformulation of the law is necessary in order that law provides a countervailing power and all the necessary safeguards (as transparency and opacity tools).

[183] *Ibid*. p. 189. According to the Hildebrandt, we need an Ambient law that is embodied in the algorithms and human machine interfaces; for this "we need to become literate in terms of a new script".

[184] An example from the side of the technicians is offered by G. Iachiello, Design by proportionality, http://portal.acm.org/citation.cfm?id=1054986.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

by Hildebrandt, the paradox of the 'Rechtstaat'- that implies that the power of the state can be contested in a court of law that is based on the authority of the state - should be translated into emerging technologies used to implement the law: "thus we may sustain the rule *of* law against the rule *by* law and against a rule *of* technology"[185].

The legal-technical approach towards new technologies for the protection of privacy rights will be discussed again at the end of this paper.

4. Detection technologies

4.1. Historical and legal context

Before taking a closer look at some of the *AmI detection technologies* and their impact on privacy and other rights, it is necessary to consider the context of countering crimes and terrorism in which they can be located as security measures: as such they constitute restrictions/exceptions to privacy right.

As mentioned earlier, most of the fundamental rights, set out in the main international acts, are not absolute, in the sense that limitations and exceptions are provided by the law. One of the main issues regarding the enforceability of privacy as a fundamental right is to identify its limitations. A clear example is the second paragraph of Art 8 ECHR that permits the Member States to apply, under specific conditions and requirements, restrictions to this right.

Evaluate whether and to which extent these limitations are permissible under HR law is one of the main issues that doctrine and jurisprudence are called to solve. Fight against terrorism has been resorted to by many States to justify their exceptions to human rights and international law. Different sorts of arguments of these unilateral exceptions pertaining to counter-terrorism have been identified, some of which, although having a valid legal basis, exceed the limits allowed in order to be considered as legitimate, or are open to abuse (seeking to deny or unfairly derogate to human rights)[186]. Doubts of legitimacy, as consequence, are extended to the measures adopted to put in practice these exceptions.

[185] M. Hildebrandt (2008c), Legal and technological normativity: more (and less) than twin sisters, *Techné: research in philosophy and Technology,* 12, 3.

[186] M. Sheinin, M. Vermeulen (2010), *Unilateral exceptions to international law: systematic legal analysis and critique of doctrines that seek to deny or reduce the applicability of human rights norms*

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

At least some of these arguments pertain to exceptions to the applicability of the right to privacy while grounding counter-terrorism measures and therefore are interesting for a study on (AmI-) detection technologies.

As it is well-known to HR and international lawyers, major problems in countering-terrorism while respecting human rights are due to the absence of a uniform and precise definition of 'terrorism', with the "risk of unintended HR abuses and even deliberative misuses of the term"[187].

The vague definitions of this term adopted by the states have often as consequence to allow states to label-and pursue- as terrorist persons or groups that do not deserve it, but who are dissidents with the governments: political opposition groups, non-violent separatist movements, religious people, indigenous populations, HR defenders[188].

In other words, the qualification of an action as terrorist and a person as suspect of terrorism justifies a broader use of surveillance powers. The risk is evident that counter-terrorism measures could be adopted against these categories of persons, including investigative and detecting measures that rely on - more or less - 'soft' and intelligent technologies[189] (see below), or simply placing, for instance, more cameras in contexts of political protests (see Perk case in UK)

Given the lack of an agreed definition of terrorism (or related term such as 'state of emergency' or 'national security'), an anchor in the evaluation of a definition of terrorist complying with HR, is provided by the legality requirement that any national definition of crimes must meet, *ex* art 15 of the ICCPR; this

---

in the fight against terrorism, EUI Working papers, Law 2010/08, European University Istitute, Florence. The types of unilateral exceptions *ivi* discussed, through a systematic approach go from 'the denial of the applicability of human rights law during armed conflict' to 'the denial of extraterritorial effect of human rights', or 'withdrawal from treaties'. The authors stress that these limitations often relate only to a specific treaty or procedure but do not affect the substantive obligations of the States under international law: the derogation to a treaty norm, for example, does not exempt the State from the correspondent obligation under customary law (due to the broad overlap of the two orders of law). The main problems remain, hence, on the procedural level, that these exceptions/constructions preclude the regular monitoring functions by HR courts or treaty bodies.

[187] M. Sheinin, M. Vermeulen, *cit*. p. 2.

[188] Potential risks of deliberative misuse of the term terrorism/terrorist - especially by the oppressive regimes - seem to come also by interpreting the calls for action from the UN Security Council as leaving the states to define by themself what terrorism is: examples are the UN Resolution S/RES/1373 of 2001, adopted immediately after the 9/11 attacks and containing the list of mandatory measures to be taken by the states and the recommendations of the Counter-terrorism Committee of the Security Council. The definition contained in the European Council Framework Decision on terrorism also seems inadequate according to the EU Network of Independent Experts on fundamental rights, *The balance between freedom and security in the response by the European Union to the terrorist threats*, May 2003, quoted by M. Sheinin and M.Vermeulen, *cit*, p.3, who claim that legal definitions of terrorism should refer to the methods used not to the aim or to the author of the acts and should refer to a pre-existing-defined- crimes.

[189] The term intelligence in English is ambivalent, in the sense that it refer both to one of the governmental branches and to a high level of reasoning capability of computers. After all, all the ICT revolutionary innovations, as in the case of Internet, started in military or security context.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

provision contains the rules of law, essential in a democratic society, of *nullum crimen sine lege*, of *nulla poena sine lege* and the requirements of accessibility, precision and foreseeability of the law[190].

These requirements might be invoked not only to avoid abuse in the criminalization of actions and opinions, but also to avoid a sort of anticipation of the punishment, or of the judgement that could pass through the use of new *detection* and (for definition) 'preventive' technologies (see *infra*)[191].

Regarding the possible exceptions to the right to privacy in the name of the fight against terrorism, it seems that the major concerns derive from the (1) 'unfair derogation during a state of emergency' and from (2) the 'overly broad use of limitations allowed by HR treaties'[192].

1) Contrary to rights that do not admit exceptions (such as the right not to be subjected to torture, which constitutes a peremptory norm) the right to privacy is a derogable norm and its acknowledgement by HR treaties goes with possible and sometimes necessary restrictions; or it falls within the possible derogations that should be adopted by states in times of emergency threatening the existence of a nation. Concerning the first reason (emergency), an appropriate adoption of measures that derogate from HR should, therefore, not only base on a state of emergency officially proclaimed, but be also *necessary* and *proportionate*, i.e., keeping the derogation to a minimum and remaining within the exigences of the concrete circumstances. Examples of lawful measures/derogations of rights such as free movement, peaceful assembly and the right to privacy are checkpoints on the roads, restrictions on mass demonstrations or inspections of correspondences[193]. What, instead, should be judged as unlawful is the unfair prolongation of the state of emergency by some states endeavour to pass off extraordinary measures as normal[194].

[190] M. Sheinin, M. Vermeulen, *cit*. p.5.
[191] As testified to by privacy activists (see below EPIC on body scanners) technologies already in use as surveillance measures are able to invade and humiliate, in some cases, the persons subject to controls. It could be said that they operate a sort of unjustified threatment that sounds like a punishment and should therefore banned or at least well pondered before adoption (in this case an important role could be played also by the national Authorities for privacy protection).
[192] See for the other exemples of unilateral exceptions M. Sheinin & M.Vermeulen, *cit*. p. 5.
[193] *Ibid*. p. 22. Examples of derogation clauses are art 4 ICCPR and art 15 ECHR.
[194] M. Sheinin & M.Vermeulen, *cit*., write: "An emergency measure […] must be termporary by definition, the aim being exactly the restoration of normalcy, including the full protection of human rights […] derogations should be seen as a particular form of restrictions upon human rights rather than as their temporary circumvention", noting also the risk that, after the 9/11, terrorism becomes one of the most common reasons for a prolonged state of emergency.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

It can be assumed that these criteria should be taken into account also to evaluate the lawfulness of counter-terrorism measures relying on refined technologies of collection, extraction and automated processing of data, biometric profiling extension and in general other detecting technologies such as those indicated below[195].

The absence of a clear conception of emergency can have negative consequences on the respect of HR (thus also on privacy rights) that could especially derive from an incorrect use of the margin of appreciation left to the MS. As some authors observed[196], the necessity and proportionality scrutiny that the Court reserves to itself, should be a serious and well thoughtful process rather than the simple balancing between rights and security, enable to establish when derogations to human rights actually increase security or if, instead, other less 'infringing' measures can be used[197].

As we can observe a sort of trade practice in commercial privacy (personal data for economic benefits, in the so called 'gift economy'), we can also acknowledge a dangerous practice of a trade-off of privacy for security [198].

2) The other form of unilateral exception to HR that states would found on counter-terrorism reasons and impacting on privacy is the excessively broad use of limitations, since in the aftermath of 9/11 the increasing concerns for security have caused a revaluation of the balance between liberty and security, in the sense of reducing civil liberties in order to ensure more security[199].

4.2. Counter-terrorism practices and conditions for privacy limitations

[195] *Ibidem*, p. 23, in which appears that, after Israel, U.K. is the state that decleared more times and manteined the longest a state of emergency, derogating to several HR obligations. As a matter of fact, the main criticized detection technologies are in use in these countries (see below).
[196] De Hert (2005), *cit*. p. 86; De Beer *et al. cit*. p. 156.
[197] Moreover, it has been noted that the vagueness of the term 'emergency' have already allowed (and can do it more in the future) an unacceptable extension *per analogia* of the derogations (through the argument of the terrorist as *hosti humani generis*) and the unfair use of the necessity defence as a state policy: see Sheinin and Vermeulen, *cit*. p.25.
[198] See De Hert, (2005), *cit*. See also K. Roach. (2006), Must we trade rights for security? The choice between smart, harsh, or proportionate security strategies in Canada and Britain, *27 Cardozo Law Review*.
[199] Against these doctrines are, among others, the former UN Secretary General Kofi Annan and the European Parliament. See EP Resolution of 25/11/2009 on the communication from the Commission: "security must be pursued in accordance with the rule of law and subject to fundamental rights obligations" , quoted by Scheinin and Vermeulen, *cit*.p. 26, who enphasize the lack of incompatibility between HR and security and the mistake in trading-off human rights and security, since the security must be ensured in an HR framework.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

The risk of progressive erosion of privacy deriving from an inappropriate balancing approach[200] - as shown from the adoption by several Member States of new legislative measures seeking to reduce the excessive weight to privacy in counter-terrorism practices - has been addressed by the 'Special Rapporteur on the protection of human rights while countering terrorism'[201]. In particular, in his Report it is discussed whether a fundamental right as privacy should be just considered as a factor of the balancing process or whether it is possible to talk about a HR framework that provides the instruments for this weighting: in particular the test of permissible limitations and the criterion of proportionality.

Permissible limitations, necessary *and* proportionate, in fact, are prescribed in relation to human rights, like privacy, for legitimate aims (that can be founded for instance listed in the norm that protects the right - Art 8 Conv): consequently the pondered decision by a state to restrict a right must remain an exception and respect the main rule (*ratio*) enshrined in the related norm that protects the right in question', such as art 17 of ICCPR.

This implies that, although privacy is a derogable right, the fact that it is subject to permissible limitation "should be understood to include one or more essential elements that crystallize a broader principle into a rule that allows no limitations or balancing" [202].

Therefore, the essential core of privacy, as well as of other rights, should be respected in its scope of application. The importance of this assumption is not only evident in relation to the practice of extending the balancing to absolute rights (like some doctrines would) but also with regard to derogable rights, since it allows to take into account and respect the non-derogable dimensions of them.

Therefore, concerns regarding the protection of privacy right in the fight against terrorism are not only justified but call for a more thorough check of the related limitations.

In other words, even the right to privacy should be subject to a rigorous limitations test, since the interest of public security in the fight against terrorism can

[200] Etzioni A. (2002), Implication of Select new technologies for individual rights and public safety, *the Harvard Journal of Law and Technology*, vol 15, n. 2 and, of the same author (2004) DNA tests and databases in Criminal Justice: individual rights and the common good in D. Lazer (eds.) DNA and the Criminal Justice system: the technology of Justice, *MIT Press*, p. 197; See also G.Vermeulen &W.De Bondt (2008), Finding the right balance between effective measures and fundamental rights guarantees, 79 *Revue internationale de droit penal*.

[201] See the Report of the UN Special Rapporteur (2009) A/HRC/13/37, *cit*. p. 9.

[202] M. Scheinin & M. Vermeulen, *cit*. p. 27.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

(and actually does) legitimately require restrictions to privacy right, which are, nevertheless, permissible if they remain within the parameters set by HR law[203].

As argued by the Special Rapporteur on Human Rights and counter-terrorism, in order to assess the permissibility of the restrictive measures, the same should satisfy a set of conditions, which constitute the legal safeguards to measure and ensure, by the States, the necessity, proportionality and reasonableness of the interferences [204].

These conditions, that are particularly relevant also for the assessment of (AmI) detection technologies used in the counter-terrorism context, are:

a) no restrictions to the essence of privacy right;

b) any restrictions should provided by the law;

c) restrictions must be necessary in a democratic society;

d) any discretion in the implementation of the measure should be scrutinised: to a deeper intrusion should correspond a stronger judicial review;

e) it is not enough that the measure serves one of the enumerated legitimate aims, since it must be also *necessary* for reaching that aim.

f) restrictive measures must be *proportionate* to the interest to be protected and appropriate to achieve their protective function; that implies that they should be chosen because they are the least intrusive among those that could achieve the desired result.

The last criterion is particularly relevant especially in the assessment of new refined technologies, that are often chosen because the most efficient or because respondent to market logic or scientific research outputs[205].

4.2.1. Impact on other related rights

[203] Practice has shown that states justify their measures against terrorism as imposed by their legal obligations under the UN Charter (in particular, under the Security Council's power to impose upon Member S mandatory measures). As enphasised by M.Sheinin and M.Vermeulen, *cit*., p 12, there is no contraddiction between human rights and the UN Charter, and the counter-terrorism measures, even when adopted on the basis of mandatory resolutions - such as the SC Resolution 1373(2001)- must be implemented in full compliance with HR.

[204] See the Report (2009) of the Special Rapporteur for HR *cit*. p. 7, in which we can read: "article 17 of the International Coventant on Civil and Political Rights, is flexible enough to enable necessary, legitimate and proportionate restrictions to the right to privacy and should be interpreted as containing elements of a permissible limitations test".

[205] See the discussion on the relevance of subsidiarity criterion as support to the principle of proportionality, infra. One could argue that seen the sophisticated technologies available, such as biometric behavioural sensors, people could feel less the intrusiveness. With the *Marper* case (see below), the Court gave in its reasoning some elements to be convinced of the contrary, and it based them on the possible risks for the relational dimension of the right to privacy.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

A'legal black hole' is perceptible - similar to that invoked in humanitarian law by some governments to justify their treatments of suspected terrorists[206] - in the lawfully - questionable use of new detection technologies towards suspect people (see *infra*); since their use has been broadly extended, so much to make all citizens potential suspects, it may be noticed a legal black hole in HR protection, at least in places and moments where these technologies are used (airports, etc.). A gap that could be even more difficult to distinguish and to contest in a pervasive computing world.

An important issue is that these measures while breaching the privacy right have an impact also on other fundamental rights, such as free of movement, due process or freedom of expression. Free movement rights may be easily affected by surveillance measures, through watch lists, tracking devices, insidious scannerns and through extended data collection, on the basis of which are create profiles to be matched easily with even remote lists of suspects or other different sources belonging to different entities/owners/responsible parties.

In this context, it is difficult or impossible for the individuals even to know about these profiles and, even then, to contest the decisions taken by the authorities on the basis of them, not only because they are foreign in foreign countries, but also because the profiles are often generated by complex processes of data-mining (i.e. extraction of knowledge, through algorithms, from data bases), difficult to understand and to contest, with a serious infringement for their right to due process.

Algorithms[207], then, are going to be weighed and 'believed' more than and in spite of the declarations of individuals and can arrive to identify innocents as criminals. The complex and 'secretive' nature of the surveillance measures, and in particular of those relying on automated technologies (algorithms), in fact, makes difficult or impossible a demonstration of the unjustified situation of surveillance and the unlawful interference in privacy right or the unlawful violations of data protection. The result is that subjects could be denied access to justice (Court)[208].

Hence, protection of the right to privacy could be seen as an instrument to protect also other rights and represents therefore an essential value of a democratic society.

[206] See, among others, S. Barelli, Casting light on the black legal hole: International law and detentions abroad in the 'war on terror', *International Review of Red Cross*, n. 857, p. 39.
[207] See K. Vries, *cit* p. 71.
[208] Report of the Special Rapporteur, *cit*., p.15.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

4.3. 'Permissible' detection technologies in light of HR

The growing interest in the described new surveillance technologies[209] is precisely due to the fact that these technologies have enhanced the ability of the governments to develop record-keeping instruments, and refined instruments of control with the possibility to endanger the privacy and other related rights. This is also the reason for the parallel development in many countries of data protection principles, (initially interpreted only as included in the right to privacy), but also becomeing the elements of an autonomous fundamental right to be respected in all the practices that involve personal data-processing for private or public aims. As just said, there are situations in which States can legitimately limit the right to privacy and countering terrorism is one of them, for the aims of which security agencies can investigate and check persons (or personal belongings), also with new technological systems, as well as share personal information among each other.

Countering terrorism, nevertheless, does not legitimate all the interferences in the private sphere of individuals, which should be, on the contrary, well evaluated, and the same should be for the surveillance measures eventually used to achieve the aim[210].

---

[209] Examples of research projects that testify to an increasing attention for these topics are: Detecter http://www.detecter.bham.ac.uk/ ; Prescient, http://www.prescient-project.eu/prescient/index.php (EU), and Fredom, Security and Technology of the CDT http://www.cdt.org/issue/security-surveillance (U.S.).

[210] See G. Van Der Schyff (2005) *Limitation of rights,* Wolf Legal publisher, Nijimegen, p. 228. The Court of Strasbourg's case-law has shown different approaches to the identification of the protected conducts and interests and their limits. Especially with regard to the rights presenting a two-stage structure (whereby, as in art 8 or art 11, the protected right is stated in the first sub-section, followed by the requirements that *justify* a limit to such protection in the second sub-section) the Court adopted sometimes more narrow interpretation while in others preferred a wider approach to the identification of interference with a right. In *Klass v. Germany* of 6/09/1978, for instance, it was found that the complained system of surveillance affected all users and *potential* users of the telecommunications services: as such surveillance implies a restriction of free communication, therefore interferring with the right enshrined by Art 8. In this case, the Court stated that the simple existence of a system of surveillance is a 'menace' and sufficient to constitute an interference with the private life.
In the same case, the Court (although generally willing to attach importance to the purpose of national security) stressed that the state did not enjoy an unlimited discretion in engaging in surveillance, as that would threaten to undermine democracy: if the importance of the purpose of national security is dictated by the need to protect democracy, it is also to protect the latter against the mere measures designed for its protection.
On other occasions (*Dudgeon v. U.K.* 22/10/1981, Publ. E.C.H.R. Series A, n. 45) the Court even recognized this interference in the mere existence of a legislation (although the absence of a measure of implementation) that would criminalize homosexual conduct, directly affecting the applicant's private life. Differently, a narrow interpretation of what constitutes an interference with the protected right has been adopted by the Court elsewhere; in *Van der Ven v. Netherlands* of 04/02/2003, the Court recognized that *some measure of control* (over prisoners' contacts with the outside) is not in *itself* incompatible with the Convention. As stressed by Van Der Schyff, *Ibid*. p., 74, this *dictum* is to be rejected, since, considering the measures in *themselves* compatible with the Conv., "it presupposes that the internal nature of rights, their abstract quality, is to be the only guide in their application"[…] "confusing between a *factual* interference and a *justified* interference leading to an interference being justified at the first stage of the inquiry".

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

For this reason, criteria for permissible limitations derived in particular by the interpretation of art 17 of CCPR (as the most important international legally binding provision on the fundamental right to privacy), have been identified[211] and should be taken into account by States and security agencies when adopting security measures, including (new) detection technologies.

Possible surveillances activities put in place in the context of countering-terrorism after 9/11, that rely upon existing or new technologies, range from covert surveillance to identify illegal conduct, exchange of data among intelligence agencies, interception of communications by intelligence and law enforcement agencies, targeted surveillance of individuals to build a legal case (there should be a factual basis which justify the suspicion of terrorist act) to spyware installed in suspects' computer to allow a remote computer access.

New initiatives have been adopted by governments to identify, check, track with new sophisticated technologies even larger numbers of ordinary people[212].

As mentioned earlier, biometrics appear able to facilitate, in automated way, these activities; biometric measures became a key element in surveillance activities (facial recognition, fingerprinting and iris-scanning) and it is reasonable to expect their increase in an AmI world: special concerns for privacy right seem to derive from their storage in central databases, in which more risks of unauthorized access, abuse or error rates are high as well as of false positive and fraudulent use[213]. The consequence could be in a stigmatization effect of people suspects or in wrongful criminalization and social exclusion of individuals[214].

---

[211] Report of the Special Rapporteur *cit*. p. 9.

[212] As noted by the Special Rapporteur *cit*., p. 10, when extended to larger group of people the surveillance is typically subject to a weaker regimes of authorization and oversight HR standars do not seem to be respected in many cases of 'stop and search': there are serious concerns in terms of racial profiling and discrimination and of the breach of the proportionality requirement: see Open Society Justice Initiative, http://www.soros.org/initiatives/justice/focus/equality_citizenship/articles_publications/articles/ethnic profiling_20060629).
Among other factors that enter in the "justificatory exercise" of the limitations of rights, proportionality is of a special significance. Summarising with Van der Schyff, cit., 216, it "is a tool with which to decide whether relevant and sufficient reasons have been given for an interference against the background of a democratic society, thereby proving the presence of a pressing social need- and thus the necessity of limitations".

[213] See case *Marper v. U.K.* , *cit. infra*.

[214] Another technique is the watch-list monitoring (like no-fly lists) for terrorism aims. The main concerns come from the data integrity and risks of errors, that could not be solved easily because frequently kept secret: subjects are continuously under surveillance without knowing it and without an independent oversight. The no-fly lists deserve to be considered in an AmI discourse especially if we think that these lists could be used in connection with profiling techniques of a complex pervasive computing system (also by private companies) for denying access, services, jobs.
Data protection principles are also at stake regarding this techique, for the practice to reuse the lists for different purposes and to share them with other institutions without the consent of the subjects;

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Another security practice put in place in response to the terrorism concerns, that seems to lead not only to privacy breaches but also to increased limitations and monitoring of the movement of people, is the augmented resort to checkpoint and border control.

It must be noted that the technologies used as security measures for this scope could be of a different nature and they normally involve advanced and sophisticated technologies, included of AmI nature (biometrics, sensors, etc.). These devices, together with data-sharing agreements[215] allow governments to create very precise profiles of travellers in order to identify patterns that correspond to those of terrorists[216]. Therefore, the result of a database query (that, presumably, will be soon easily controlled by an automated system of biometric sensors)[217] may condition the freedom of movement of people, without due process[218].

Beside the risks linked to wider data collection, the private life of individuals is threatened by the further, even more invasive, screening practices (as shown by the new body scanners - see below).

Moreover, increasing measures of migrants monitoring gives rise to concerns for right to privacy and also for other rights, as non-discrimination, due process, free movement, freedom of association and other specific migrants rights (contained in migrants treaties)[219].

Increasingly, additional information is required of the travellers and is often used for different purposes: counter-terrorism measures oblige the individuals to give many information otherwise kept private and provide law enforcement officials with more powers to obtain information in their investigations[220]. This brings in some

---

moreover erroneus information can be used to take decisions on individuals (that may be refused to take a plane, obtain a visa, cross a border, without having been presented with evidence of any wrongdoing (Report of Special Rapporteur *cit*, p. 12).

[215] The informations are obtained by consulting security agency databases and matching with the watch lists. See the debated EU/US agreements. On their recent developments see M. Botta & M. Viola de Azevedo Cunha (2010), La protezione dei dati personali nelle relazioni tra UE e U.S.A: le negoziazioni sul trasferimento dei PNR, in Diritto dell'informazione e dell'Informatica, Giuffrè, Milano, vol. 26, n. 2, p. 315.

[216] See the concept of pattern recognition in M. Hildebrandt (2008b), *cit*, *infra*.

[217] See DETECTER project, *cit*. and for the potentialities offered by sensors see the project *Sense*: http://www.sense-os.nl/.

[218] Report of the Special Rapporteur, *cit*., p.12.

[219] It must be noted that foreigners might not be granted equal access to judicial remedies and rights at the borders are usually significantly restricted. *Ibid*. p.12. Concerns, under the right to privacy and other migrants rights, seem to derive also from the extended use of the informations gathered under migrant law (asylum seekers, illegal immigration) for the prevention, detection and investigations of terrorist acts, as expressed by the EDPS on Eurodac, in April 2010, and on the Revision of FRONTEX's mandate in May 2010.

[220] *Ibid*. The author mentions the example of access to travellers' laptops without judicial authorization. See also the US Department of Homeland Security, Privacy impact assessment for the

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

countries to the possibility for law enforcement authorities to obtain more easily the disclosure of data originally collected for journalistic, commercial or whatever other purposes[221].

4.4. Some applications of detection technologies and related risks for privacy

As said before, many recent post-9/11 surveillance strategies, in and outside Europe, seemingly go in the direction to introduce the new forms of surveillance technologies, incurring criticism from civil society[222] .

Refined technological measures for security purposes have already been adopted, as *detection technologies*; others are currently being tested relying on biometrics and modern body scanners[223]. As mentioned earlier, many of them constitute the basic technologies that will form the architecture of an AmI world, a fact that would alone justify the concern about (and interest in) possible *AmI detection scenarios*.

Examples of detection technologies (hereinafter DT) go from more 'simple' and 'old' technologies such as CCTV (closed-circuit television) in public spaces, to full body scanners, substance detectors, covert cameras, phone and internet monitoring, location tracking and data-mining techniques. It is not difficult to imagine that privacy risks, arising from these security technologies, vary from one application to another, and the more complex the system (i.e., involving a variety of techniques), the more privacy rights are in danger.

Since complex technological systems are likely to be used in what can be called an '*AmI detection scenario'*, the considerations made about the dangers of

---

border searchers of electronic devices, 25/08/2009 about the need to leave vulnerability in the electronic devices to allow security search, localization, tracking. It is not difficult to imagine in the near future of AmI how this search could be interconnected with remote databases/profiles and controlled automatically.

[221] See Report of the UN Special Rapporteur, *cit.* p. 14. This trend towards data-mining and 'data merging' of different nature and of purposes could be also noticed in both directions (security vs commerce contexts and *viceversa*). It would be, hence, not hard to share the Gandy & Schiller's concern that "the use of data-mining in the so called 'war against terrorists' will soften us up for its use in the war against the global competitors." See O. H. Gandy & H. Schiller (2002).

[222] See EPIC, the Electronic Privacy Infromation Center, http://epic.org/.

[223] An idea about how 3D whole body scanners work is given by J-M Lu & M-J. Wang (2008) Automated anthropometric data collection using 3D whole body scanners, Expert System with application, 35. Although the automated data collection and human body measurements (through *ad hoc* algorithms) are presented there as an efficient tool for health or pruduct design, the article is another clue of the extending application of algorithms in everyday life and of a trend of both corporate as well as public governance, in which we can read: "With the growing trend of globalization, the concept of mass customization in product desing is becoming an important issue[…]. Since the developed system is fully automated and easy to use, many applications can be extended".

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

these detection technologies –separately and combined- should be taken into account.

In the taxonomy developed by Guelke &Sorell[224], different types of harms - *intrusion, error and discrimination, chilling effect* - as consequence of the several risks raised by the use of these DT are identified.

It can be noted with Guelke & Sorell that the intrusion in the right of privacy deriving from the different DT technologies can be multifaceted: invasion of home spaces, of the zone covering the body[225], invasion into private life (deemed as including individual conscience and opinions) and accessibility by further subjects[226]. At the same time, the risks of DT in producing mistakes are, as well, relevant for the indirect outcomes in terms of privacy and discrimination rights: the data acquired could be itself prone to false positives/ambiguity; an unjust decision (and a sanction) on an individual could be based on the errors generated; mistakes can result from the same storage of information (for example, because recorded incompletely).

The different DT applications may clearly have different outcomes: while the greater risk of intrusion is mainly linked to body scanners and Internet monitoring, error and discrimination seem to derive mainly from cover cameras and data-mining[227]; the 'chilling effects' are instead common to most of them[228].

---

[224] Guelke & T. Sorell, *Detection Tecnology Survey n. 5* for the DETECTER project - D12.2.5 of the 02.06.2010, available at http://www.detecter.bham.ac.uk/.

[225] Two key examples are represented by the so-called 'technological strip search' (millimetre wave body scanners) and 'technological property search' (portable thermal imaging cameras), the first threating the inegrity of the body, the second the inviolability of the home; about that, see B.J. Koops & M. Prinsen (2007), Houses of Glass, Transparent Bodies: how new technologies affect inviolability of hte Home and Bodily Integrity in the Dutch Constitution, *Information & Communications Technology Law*, Vol. 16, n. 3, Routledge, and G. T. Marx (2002), What's new about the 'New Surveillance'? Classifying for change and continuity, *Surveillance & Society*, 12. See on thermal detection devices *Kyllo vs United States* 533 US 27,121 S Ct 2038, in which the Court stated that the police could not use these devices without a warrant to search a house – although one of the reasons alleged by the Court was that the technology was not in *general public use* (emphasis added).

[226] Many are for examples the risks of intrusiveness arising from the use of body scanners; concerns come in particular from the millimeter wave BS, which reveal a clear image of naked body (but see the passive type of 'cookies cutter' and the minimal intrusiveness of scanners that detect a dangerous substance only). Especially after 9/11, the technology is being deployed in a variety of locations in the absence of legal guidelines. See B. Bowling et al. cit. 61. Risks of unauthorized access to stored information collected through body scanners are also high, as well as the sense of invasion - as denounced by EPIC and by some celebrities, fearing for the sale of their images on the black market. It is, however, difficult, as stressed by Guelfe & T. Sorell, *cit.*, p. 22, completely to rule out the possibility of images on computers from being surreptiously recorded. A further risk coming from the new sophisticated scanners is to acquire extraneous (i.e. more than is sought) and even sensitive, information about the subject; this also in case it is a vehicle to be scanned.

[227] As observed in the by Guelke & T. Sorell, DETECTER, *cit.* p. 21, if intelligence is recorded, widely shared and acted upon the various sources of errors may result in significant sanction: a significant example is no-fly lists; if intelligence is recorded incompletely, suspicion may be registered without adequate opportunity for correction; moreover, dataming may spread suspicion on

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

In the assessing the impact of (AmI) detection technologies on HR, the afore-mentioned risks must be taken into account: obviously invasion and discrimination), but, considered the afore-mentioned discussion on the 'meta-rights' (see *supra*, Rouvroy) highlighted by the deployment of surveillance technologies and of a precautionary state, also the chilling effects on legitimate behaviour (such as free association, free speech, political organization) are relevant[229].

Some risks incurred by detection technologies that are basic in AmI – cameras, scanners, biometrics - are those that Guelke identifies in *mission creep and 'use creep'*: the first term indicating that DT established for a particular purpose could come to be used for further (different) purposes; the second, meaning that, if a device is conveniently used for a specific purpose usually results in an expansion of its use[230]. One could argue that these risks have already their legal answer in the purpose limitation principle; but, as Guelke exemplifies, the effectiveness of this principle is often jeopardized by manifold use of detection technologies, thus, the gradual costumization of people (and legislators) to the presence of new, multifunctional technologies turns out in gradual erosion of privacy and autonomy of people.

A taxonomy of the harms for privacy (and related rights) such as that suggested by Guerke in the DETECTER project, as argued by Solove, could help to focus directly on the problems and therefore to find more suitable solutions.

---

large number of innocent people, targeting, often disproportionately, members of particular social or cultural groups.
Concerning the level of invasion in private life using datamining, it is clear that it is more invasive the more information that is aggregated and the more people who have access to it.
It is possible to argue that a complex scenario, such as of AmI, will face all the issues regarging the different types of detection technologies involved, requiring, hence a systematic approach in proving the necessary safeguards (technological and legal).

[228] For 'chilling effect' is meant any practice (or law) that has the effect of seriously dissuading the exercise of constitutional right; see http://law.jrank.org/pages/5198/Chilling-Effect-Doctrine.html">Chilling Effect Doctrine.

[229] See the J. Guelke & T. Sorell Survey n. 4, D.12.2.4, p. 3. In particular there is a chilling effect on the individual will to take part in public activities, to act or speak freely in spaces covered by video and audio surveillance, scanners, phone and Internet monitoring; also the use of databases by government might disincentivise behaviour that could likely match the profile of someone pursued by the authorities (see Survey n. 5, p. 28).

[230] Examples of the risk of 'mission creep' are: cctv cameras installed for one purpose come to be used for another one; vehicle-trackers or (especially) computer monitoring and the information gathered, could come to many uses other then detection; data-mining from databases is particulairly given to find different types of target; given the amounts of personal data that a biometric technology can reveal, could be used for further application. Examples of the *use creep* risk could be found in the proliferation of cctv, as people become accustomed to its use; in the fact that scanners easy-to-use are likely to be deployed more and more; in the likelihood that dataming techniques, as their invasion is unfelt, are used for other searches (J. Guelfe & T. Sorell Survey n. 4. *cit*., Taxonomy of harms and risks).

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

This taxonomy could be extended, for what concerns this study, by adding the risks possibly deriving from the creation of a complex 'AmI detection scenario': in a simple example, we can think about body scanners relying on biometric systems connected in real-time to (behavioural) profiles (that already alone may reveal more sensitive data than what sought, such as ethnicity, probability of illness, etc.), obtained, in their turn, by data-mining techniques[231]. The system may not only reveal more information than necessary, even sensitive, but could easily match different data from different sources, providing (supposed) complete profiles on a person or a group (living for example in a certain 'risky' area), with consequences in terms of more *unnecessary* intrusiveness into people's lives [232] and indirect discrimination (again unnecessary)[233].

Even if new technological measures are said to be effective and multifunctional, it does not mean that their deployment, especially for public aims, is a compulsory duty for our governments. Their adoption is a policy choice, but as far as their use constitutes an interference with fundamental rights, it must pursue a legitimate purpose, i.e. a legitimate goal in a democratic society[234].

As noted by Van der Schyff, it does not suffice to justify interference by simply considering the nature of the right at stake as well as the importance of the purpose pursued and the nature of the interference, "without questioning whether *less restrictive means* could have been employed in limiting the right". In other words, "not an interference as such must be evaluated, but also its relation to other possibilities in securing the legitimate purpose being pursued"[235].

---

[231] See De Hert (2008b), *cit* p. 71.
[232] See B.J. Koops & M. Prinsen (2007) *cit.* p. 178.
[233] This, without mentioning the negative consequences coming from the risks of false positive/false negative (Reports on face recognition software claim that it is unrealiable http://rinf.com/alt-news/contributions/mick-meaney/police-report-face-recognition-cctv-unreliable/790/) and of abuse of the technology or the data obtained (the side-effect of placing viewers of body scanners in a separate room is that is makes oversight of the operators more difficult, as stressed by J. Guelke, p. 23).
[234] As stressed by Van Der Schyff, *cit*. p. 185, the identification of legitimate purposes that may be pursued in limitating one of fundamental rights can be identified expressly in specific provisions (it is the case of the ECHR, art 8 (2), in particular; ICCPR, art 17) or in a general limitation provision (as for the UDHR, stating that rights may be limited in the interest of the 'general welfare of a democratic society' or, in other cases, it must be derived from the values that ground a democratic society. It can be said, however, "that the general welfare of a democratic society is the broadest and most inclusive legitimate purpose that may be pursued in the limitation of rights" and that all the various purposes contained in specific limitation provisions can be traced to the notion of general welfare of a democratic society. National security is considered as one of the category of this general interest, and an important purpose in the limations of rights. See cases such as *Leander v. Sweden* or *Klass v. Germany*, in which a surveillance system was justified in the interest of national security.
[235] G. Van Der Schyff, *cit*. p. 147.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

It is, hence, in respect of the requirement of necessity for a democratic society, defined through the criteria of proportionality and subsidiary (see *infra*)[236], that the margin of a legally-*tolerable* detection technologies should be drawn, also in a 'smart' – detection - environment.

4.4.1. The gradual expansion of Full Body Scanners and the increasing concerns for HR

Among other detection technologies, the expansion of new body scanners are receiving today a special attention by the public opinion, since they are being adopted in the major airports around the world (U.S., Israel, Europe). Their gradual expansion is strongly criticized by privacy advocates in particular in U.S., and has given the impetus for legal claims. One of the major civil liberties group, EPIC,[237] recently filed (August 2010) a lawsuit against the DHS of the U.S.[238], objecting in particular its 'Whole Body Scanners program' and urging for the suspension of the same[239].

After the U.S. Transportation Security Administration (TSA)'s announcement of a proposal to deploy a whole body imaging machine[240] and the consequent petition for its review filed by EPIC, the state agency claimed that the machines were safe, effective and consistent with Americans' constitutional rights (referring in particular to a new type of detection means, the 'backscatter X-ray' body scanner, based on the emergence of radiation from the surface of a material and able to produce photo-quality images of travellers as if they were undressed); the same TSA stated that the raw images will be deleted, but, according to EPIC, the problem is that there is no law that prevents the TSA from saving the original, detailed images. EPIC

[236] See De Hert (2005), *cit*., p. 93: "it is intended to put sensibile limits on privacy-infringing procedures[…] Privacy infringements would only be possible if there is no other means to safeguard the public interest in a less-invasive-to-privacy way". Van Der Schyff, cit., p. 212, quoting the *Sunday Times v. U.K.* case, notes that the ECHR equates necessity with a 'pressing social need', but also that the term is a relative concept, taking its meaning from the context and being applied by balancing competing factors, such as proportionality and the margin of appreciation.

[237] EPIC (Electronic Privacy Information Center), *Whole Body Imaging Technology and body scanners,* http://epic.org/privacy/airtravel/backscatter/

[238] Privacy Group Files Lawsuit to block airport body scanners, R. Yu, USA today, 13.07.2010.

[239]See EPIC vs DHS (Suspension of body scanner program, 18.08.2010) available at http//epic.org/privacy/airtravel/backscatter/.

[240] V. Pop, *US Outstrips Europe on body scanners*, Business Week, 23.06.2010.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

contests in the lawsuit that, in case of use of this technology for airline passenger screening, the registered image is particulary invasive [241].

It can be argued that the main concerns for privacy derive from this technology's capability to detect even the intimate figure of a person (therefore a synthetic image, a 'mannequin' solution, should do not generate the same issues), while their relevance in an AmI discourse is justified by the fact that many of their features and functionality (use of sensors, biometrics, real-time processing) and, more important, their possibility to be automatically linked with a network of databases[242], are common to an AmI world.

An interesting aspect of many new surveillance technologies is that the main idea accompanying these proposals for new body scanners, is to reduce the 'hassle factor' (EPIC) while reducing security threats, that is, focusing security resources on 'suspicious travellers' reducing meanwhile inconvenience for most people[243]; the question is who decides which travellers are suspicious, and how is this assessment to be made?

EPIC opposes the expansion of the new body scanners questioning: "can the goal of safe air travel be reached without reproducing digital images of passengers' body?" According to American security experts, current technology can successfully detect dangerous materials, weapons, without resorting to X-ray imaging of passengers. As noted by EPIC, if x-ray body scanners cannot be a solution (only eventually a deterrent), since, as recognized by security experts, it is impossible to eliminate all threats to airline travel, is the effort to deter terrorists worth of the trade-off in passenger privacy?

They can be shared the concerns of EPIC that the use of body scanners could be extended to other offences rather than terrorist threats: in fact, there has already

[241] See EPIC, *Whole Body…cit.:* "The resolution of the technology is high, so details of the human form (enough to show genitalia) of airline passengers present privacy challenges". Interesting also the fact that the U.S. Department considers these machines (which costs each around $100.000) less invasive than pat-down searches, a sort of 'soft' technologies (in the above sense), while EPIC describes them as a 'digital strip search', and denounces that the scanners can save the body images for subsequent viewing by any computer's monitor: See B. Bosker *Body Scan images from security checkpoints were saved by Feds*, Huffington Post, 04.08.2010.

[242] Among which, watch-lists, illegal migrants lists, lists of possible suspects, and other databases even belonging to third countries. See in this regard, the *Kadi* case, in which the European Court of Justice ruled that national courts had to review the lawfulness of international watch-lists, *Kadi and Al Barakaat Int. Fondation v. Council and Commission*, September 2008. Moreover, it is not difficult to imagine how profiles created on the basis of facial and behavioural recognition techniques, with algorithms that can rely even on racial, gender, age factors, can be matched with the profiles obtained with these scanners.

[243] As EPIC, *Whole…cit*., observed, "these technologies are unlawful, invasive and ineffective and […] since the terrorists have been known to look like most people, a technology that will capture detailed images of potentially all passengers will hardly lead to greater safety".

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

been an increased detection of non-violent criminal offences and the 'whole body scanners' are replacing the metal detectors at airports[244] (despite the earlier promises by the security agency (TSA) to keep these technologies only for secondary screening of passengers).

Criticism stems from the fact that the same devices or the images obtained could easily be used for new purposes and without legal oversight. A breach of the purpose limitation principle seems clearly to stand out from this practice (and further applications are expected in an AmI world) [245].

Moreover, as EPIC lamented, these measures have been adopted disregarding the public opinion[246], fuelling the generalized 'de-politicization' argument sustained by Rouvroy concerning the surveillance measures (see *infra*).

Meaningful examples of behaviour-detection technologies, that seek to use biometric/behaviour detectors and other typical AmI technologies for security purposes, are those adopted (or to be adopted) at Israel's airports[247]. Among them it is possible to find very few examples to which one could give a green light [248].

Most of these detection technologies, on the contrary, are warrying devices for privacy and other fundamental rights: the 'SDS' tool is presented as an automated check technology ('test') for both travellers and airport employees: "It's like a polygraph machine for catching terrorists, an automated filtering tool that can identify potential suspects; as such it avoids human selectors and human errors". The technology works like a lie-detector to monitor the psychological and physiological fear of a terror suspect and to assuage people's fears of being profiled[249].

---

[244] Airport-security plan calls for 500 body scanners in '11, T. Frank, USA TODAY, 03.02.2010; body scanner risk right to privacy says UK Watchdog, BBC, 20.01.2010. *The fight against full-body scanners in Airports*, Los Angeles Times, 13.01.2010.

[245] It is argued here, infact, that, although the scope of national security could justify a limitation in privacy protection, *ex* art 8 ECHR, it requires a strict control on the respect of the necessity principle, that (as discussed supra) should comprise the respect for purpose limitation, proportionality and subsidiarity principles.

[246] *Group concerned airport security scanners capture nearly naked images*, NBC, 05.08.2010.

[247] In an article dated the 15th of March 2010, on Israel 21.org, K. Kloosterman offers a list of Israel's top 10 technologies, starting with these words: "No one understands security better than Israelis, that's why the world's best innovative security technologies are being developed in Israel".

[248] On the basis of the description provided on Israel 21.org, Trace-Guard seems to be able to detect only harmful substances. The pocket-size ACRO-P.E.T. also looks unintrusive, allowing to avoid passengers screening: despite its name, it has nothing to do with the privacy-enhancing tools: this device looks like a pen, but 'sniffs out' explosive, and can investigate 'suspicious behaviour while in flight'; the Vigilant's surveillance systems, an intelligent monitoring system for crime prevention also appears neutral: it stays awake even if security personnel fall asleep.

[249] "The test tool" - explains the afore-mentioned article – "works as a robot, searching for cues that only terror suspects are likely to radiate". After all, a top security consultant, interviewed by the journalist, affirmed that Israel concentrates on the passengers and not on their luggage. See *supra* the reflection about the 'culture of fear' by M. Hildebrandt.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Another promising technology is the platform, created by a former soldier's company (Bellsecure) that provides real time communications between identification of people and cargo in the airport with local and worldwide authorities, i.e. a reliable no-fly list connected to a multitude of sources: it connects Homeland security, Interpol data, pictures, voice and video to create unified databases that can be managed worldwide.

Still under pilot test, but probably soon widespread, is the Biometric ViP card; the idea of these credit card look-like devices is to shorten the security line, since they contain personal, biometric information about each traveller[250].

Another device, of the Israeli company 'WeCU', uses behavioural science, together with biometric sensors to detect 'sinister intention' among travellers, blending high-tech with psychology: the idea is to collect, through the use of a sophisticated algorithm, unusual responses to the images that it provides in order to frustrate and trace suspects[251].

In the majority of the cases the general impression is that who thought to use these technological solutions forgot what should be detected, that is explosives and not persons.

From a European perspective, it appears that at least Art 8 (2) ECHR applies. On this basis, if other less invasive technologies could be used in their place, it would be possible to argue that invasive body scanners, at least X-ray type, could not be considered lawful as it fails to satisfy the principles of proportionality and necessity in a democratic society[252].

In Europe, indeed, the current scenario is not clearly defined, characterized, on the one side, by strong investments in security technological measures, as advanced body scanners, backed up also by the European Commission; on the other, by a heated debate and strong criticism coming, in part from civil liberty groups, by the European Parliament[253], by EDPS[254], by the Fundamental Rights Agency (FRA) and by Art 29 WP[255].

---

[250] See the italian ID football-fun card recently introduced by the Italian Ministry for Home Affairs, and issued by football clubs, although its scope 'should' be not countering-terrorism, but 'only' cataloguing peaceful and violent 'funs', seeking to create a class of 'official funs': http://www.interno.it/mininterno/site/it/sezioni/sala_stampa/speciali/Tessera_del_tifoso/; http://e-blogs.wikio.co.uk/cataloguing-the-football-fan.

[251] See K. Kloosterman, Israel 21.org.

[252] See De Hert (2005), *cit*. p. 93 and P. De Hert, S. Gutwirth (2009), *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, in Gutwirth et al (2009) Reinventing Data Protection, *cit*., p. 38.

[253] See the *EP Resolution RSP/2008/2651 on the impact of aviation security measures and body scanners on human rights, personal dignity and data protection*, of the 23/10/2008, adopted after the

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Only recently, the European Commission has adopted the long-awaited Communication on body scanners[256], but it seems unlikely to meet the European Parliament's concerns[257]. As it seems to emerge from a FRA's recent opinion[258], the Communication does not appear to have taken into account some relevant factors that are fundamental for the concrete enjoyment of rights (e.g., whether people should be given a choice of the screening method used; how intrusive body scanners are compared to other screening methods; whether the detection capability of such scanners enhances security in Europe).

It appears from the text of the Communication that privacy is not among the main concerns (in the introduction the reference is only to free movement and health). The risk for fundamental rights appear in the text linked to the different standards of scanners currently in use (as they are regulated at national level) [259], minimizing the relevance of criticism of the body scanners as such for interfering

---

Commission has proposed a draft regulation supplementing the common basic standards on civil aviation security – Regulation (EC) n. 300/2008. The EP noted on that occasion that the draft measure, including body scanners - far from being merely technical and having a serious impact on the right to privacy - was not accompained by a Commission impact assessment relating to fundamental rights; more importantly the Commission consulted neither the EDPS, nor Art 29 WP, nor the FRA. After one month, a Public Consultation on the impact of body scanners has been launched by the European Commission: http://ec.europa.eu/transport/air/consultations/2009_02_19_body_scanners_en.htm. In April 2010 the new Commission Regulation (EC) No 272/2009 entered into force.

[254] See the Reaction of the EDPS on the meeting of LIBE committee on recent developments in counter-terrorism policies, ("Detroit flight"), European Parliament, Brussels, 27 January 2010.

[255] See the Art 29 WP Consultation *The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection*, adotped on the 11 February 2009: "there has been no evidence presented to date to show why scanners are necessary and why existing measures are insufficient"[…] "The use of body scanners could only be considered as proportionate if an acceptable balance is reached considering on the one hand the necessity and the effectiveness of their use and on the other hand the intrusion in the privacy of individuals".

[256] See European Commission, *Communication from the Commission to the European Parliament and the Council on the use of the security scanners at the EU airports COM (2010) 311/4* of the 15 June 2010. Another Impact Assessment seems to be planned for the 2011, after which the Commission will likely come with a specific legislative proposal. See http://legalift.wordpress.com/.

[257] See the debate on http://legalift.wordpress.com/. As it has been noticed, the body scanners are usually introduced as a counter-terrorism measure, while the Communication considered them instruments to improve airport security as such.

[258] See FRA (2010) *The use of body scanners. Ten questions and answers of the 10 July 2010*, Luxembourg: publications office of the European Union.

[259] To date (September 2010), full body scanners have been introduced as primary method of screening passengers in Finland, the Netherlands and the U.K, while France and Italy have begun testing. The European Commission takes into account the existance and use across Europe of different models of body scanners (it prefers the generic term 'security scanners').This results in different rules being used across the EU and in the infringement of citizens'rights. The range of body scanners comprises techniques able to reproduce body images of the person and emitting ionising radiation as well as refined versions that neither produce images nor emit radiation. The Commission, nevertheless, recognizes "the fierce debate on the security scanners' compliance with fundamental rights', which (it recalls) are protected by the EU Charter of Fundamental Rights. Among possible ways to address data protection issues, a reference to an *ad Interim* code of practice is made in the Communication, see: http://www.dft.gov.uk/pgr/security/aviation/airport/securityscanners/codeofpractice/.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

with the right to privacy. In other words, the Communication does not subject these screening technologies to a proper test of permissible limitations, through the assessment of the necessity and proportionality of the interference[260].

Regarding the technology available and mentioned by the Commission[261], attention should be paid only to the systems that neither produce body images nor emit radiation (such as the 'Mannequin solution'). However, some criticism 'persists[262], especially because it does not emerge clearly in the Communication whether the use of body scanners should be mandatory or optional, and which technology should be considered the possible solution to the problems raised by the European Parliament.

From the AmI perspective, the document of the European Commission is interesting at least for a couple of reasons. First of all, it mentions (as threatening data protection) the capability of some screening technologies to capture and process the images of identified and identifiable persons, even blurred (medical conditions, such as prostheses and diapers) and the possibility that these images could be stored and subject to different use: "Image should only be used for aviation security purposes. *In principle*, storage and retrieval of images created by the security scanners should not be possible once a person had been cleared for not carrying any threat items", § 52 - *enphasis added*[263]. The issue of access and storage of these images is, therefore, of primary relevance.

---

[260] See the Report of the UN Special Rapporteur *cit*. p. 6; in another occasion the Special Rapporteur specified that: "the full body scanners are a disproportionate intrusion into privacy when measurs are not taken to minimize the negative privacy impact through: i) not storing any image; securing that no human person sees the original image; ii) including an algorithm in the design of the device that anonymizes the image of the person, without blur the image of the suspect items". Moreover, it is stressed that the main issues could not be limited to data protection and human dignity, but should include the central issue of the right to privacy. http://legalift.wordpress.com/2010/03/10/criticism-to-body-scanners-is-mounting/.

[261] Among the four technologies mentioned (§ 4.2 of the Communication), only the passive millimetre-wave systems (recently tested at the Palerm's airport – see: M. Lorello, *Debutta a Punta Raisi il body scanner "sicuro",* la Repubblica, 31.07.2010) are seemingly appropriate, since they form an image from the natural energy emitted by the body or the surrounding, they do not emit radiation and produce a rough and blurred body images.

[262] See the comments of T. Sorell, coordinator of Detecter project (*infra*) at http://legalift.wordpress.com/: "the Communication is less clear than it might be in recommending body scanners that produce mannequin or stick figure image[…]the technology is not identified clearly as a possible solution to these problems"; according to the information principle of Data Protection Directive, the kind of body image that might be used should be made clear. Moreover doubts are expressed on the unclear use of the *Automatic Threat Recognition* (mentioned at §57 of the Communication).

[263] As mentioned earlier, the risk of unauthorized access to and use of images is not so trivial, especially if we think about the possible automated connection of the whole screening system with remote databases and, in the near future, the eventuality for the images and data to be intercepted by other subjects' sophisticated devices, whatever it occurs *bona fides* or not (not to mention the interest that advertising companies could have in 'speaking' images (automatically revealing, for instance, medical conditions).

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Secondly, the Commission Communication refers to the *Automatic Threat Recognition*, that appears to be a typical AmI application (§57). Apart from the dubious utility of this system (that would add nothing relevant in term of detection capability to scanners with mannequin systems)[264], the solution appears to have dangerous and unnecessary consequences (in terms of HR and of security itself).

Risks could arise in particular if this form of automation of object recognition (mentioned among the possible ways to address the protection of human rights and that would 'phase out human analysis of images') will be used to carry out the interpretation of the images automatically and if automated security procedures will be taken as result[265].

As far as privacy is concerned, the automatic interpretation could be seen as favourable if the software designed to recognize the forbidden objects only displays part of the image and the location of the objects interested or even only the result of the authomated detection process (location of the object and connected alarm) to the security officer.

Moreover, it appears that threats to privacy and related rights (non-discrimination, due process) seem possible if the results of the ATR (in case it is used to reveal also detailed image) is associated with facial or behavioural recognition techniques and/or to different profiles derived from several and remote databases. Subjects are not likely to have knowledge of (and even less access to) these profiles and databases, but they could be denied their rights on the basis of matched information[266].

4.4.2. Extension of the security measures and growth of a 'culture of fear'

We shouldn't be surprised then to see the increasing investments (although expensive) made by governments on biometric security technology, not without its critics, especially given its supposed link to a certain *culture of fear*, widespread today in many countries.

[264] See T. Sorell, *cit*. at http://legalift.wordpress.com/.
[265] As noted by T. Sorell, *cit*., ATR without human checking might even be dangerous if led to an armed intervention in a crowed airport.
[266] Another element that makes the Communication interesting within the scope of the paper, is the reference (although quite vague) (§56) to 'P.E.T and privacy by design', see below.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

In a recent work edited by Hildebrandt, *Security in a Culture of Fear* [267], many attempts to control security risks are presented as resulting in several dimensions of a culture of fear, or better a 'fear of fear of *risky others'*.

The 'risky other', according to Hildebrandt, is the stranger (whatever, a potential terrorist, an illegal immigrant, a person with anti-social behaviour, an image on the screen of a CCTV camera, etc.) whom we don't recognize as being like us, whom we see as the cause of our fear, and for that reason, is somebody to keep at distance, to control and to exlcude: in other words, is somebody who poses unknown security risks that must be calculated and managed[268].

Another aspect typical of the current age of fear would be the vulnerability of the 'ordinary citizen' , invoked by politicians or media to justify precautionary and more stringent measures[269].

Moreover, the 'fear of fear' seem to ground also for a false trade-off between security and liberty, "based on the mistake that one could control security by giving up freedom, through which those who have little to lose may be forced to trade their liberty to secure the perceived safety of those who have much to lose"[270].

If we look at the detection technologies (even at those of a possible AmI world), it is not difficult to find in them all the afore-mentioned elements of a precationary approach, of a culture of fear[271]. It must be recalled that, as noticed in the Report of the UN Special Rapporteur A/HRC/13/37 (*supra*), counter-terrorism measures may constitute permissible limitations on human rights, but only when

[267] M. Hildebrandt, F. Makinwa, A. Oehmichen (ed.), 2009, *Controlling Security in a Culture of fear*, The Hague, BJU, Legal Publishers.

[268] We had an example of this high level alarm recently by the law enforcement authorities on the occasion of the Pope's U.K. visit: http://www.repubblica.it/esteri/2010/09/19/news/papa_rilasciati_i_sei_presunti_attentatori-7215257/?ref=HREA-1.

[269] As noticed by Ramsay, in M. Hildebrandt *et al.* (2009), this is an indirect admission of the failure of the authority of the state and of the existing criminal law (it fails to invest in fighting the causes of offenders' behaviour), that legitimizes in some countries the adoption of ASBOs (anti-social behaviour orders, like in U.K.) or the extended use of the measure of imprisonment for public protection (IPP). There would be a precautionary logic (nourished by the culture of fear especially of unknown threats) that leads politicians to take measures even if there is no evidence that they will be effective. On the 'precautionary approach' that seems to focus on abstaining from activities that could generate unexpected consequences, see also C. van Ooijen &S. Soeparman, *Surveillance in a State of Precaution. A discourse mediating state control and sociability*. Paper presented to the 'Challenging the Panopticon Effect' Conference, London, 13-15 April 2010.

[270] See M. Hildebrandt *et al.* (2009). According to the authors, the preacautionary approach (and the related issues of risky others etc.) seems aimed at calming the electorate rather than based on evidence of effectiveness.

[271] Interesting also the perspective, illustrated above, of the boredom generated by the images of the security technologies to those paid to watch them: we do not only live in a culture of fear but also of boredom, seen the technological repetition and intellectual nihilism.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

properly developed; therefore, a rigorous test for permissible limitations, 'rather than an all-encompassing act of balancing' is necessary.

5. *AmI security scenarios* and the ECHR. Does Art 8 ECHR still exert a 'dynamic influence' on new surveillance technologies?

In the context of this increasing use of sophisticated, 'soft' technologies as surveillance tools (of an apparently less invasive variety), that seem to solve in advance, to 'pre-empt' the balancing issue between security and privacy rights (in favour of the first), the feeling that these new technologies have an important impact on HR is widely held, especially if their social control capacity is unregulated [272].

At the same time, there is a considerable debate on what appropriate safeguards (legal, technical, ethical and so forth) should be adopted in order to ensure a 'guaranteed security system'[273].

Regarding the legal framework, although some authors [274] recognize a general satisfaction of the European system, adducing the existence of a solid legal framework for privacy (enshrined in Art 8 of ECHR) and data protection (protected by the Directive 46/95, by the Conv. 108/1981 of the Council of Europe and recently by the Charter of fundamental rights of the EU), others offer a critical assessment of the strength of the European HR framework.

Based on the evaluation of some features/limits of this framework (of the Convention and of the Court) [275], the analysis of the balancing process between

[272] P. de Hert (2005), p.70. In the Rouvroy's analysis the 'meta-right' of 'disobedience possibility' is also at stake. Some of the new technological devices for security scopes, with their preventive nature, no longer aim at prohibition or sanctioning of certain illegal or dangerous acts, but at making them *a priori* physically impossible. As the author stresses, although this 'impossibility of disobedience' would offer to the law a high level of effectiveness, it turns out in a serious harm (not only for authoritative regimes but) also for democratic society, which would be in this way deprived of the important instrument of public discussion ("mise en débat") and of judicial review of the norms. See A. Rouvroy (2009), *cit*., p 190.

[273] See among others, D. Wright *et al.* (2008); Report of the UN Special Rapporteur *cit.*; M. Ferndandez-Barrera *et al*. (2009) *Law and Technologies: Looking into the future*. European Press Academic Publishing, Florence; A. Rouvroy (2010), Detecter et prevenir, Les symthomes technologiques d'une nouvelle manière de gouverner, *Etat des droits de l'Homme en Belgique*, Aden, Brussels.

[274] See F. Sudre (2005), *Le droit ou rispect à la vie privée au sense de la Convention européenne des droits de l'homme*, Bruylant, Brussels; Y. Poullet (2005), *Directive 95/46: ten years after,* in Proceedings of the XXVII Internet Conference of the Data Protection Commissioners, Montreaux.

[275] P. de Hert (2005) *cit.* p. 71. Though recognizing the importance as a basic document of European human rights framework that instituted a judicial procedure allowing individuals to bring actions against governments, de Hert stresses, in particular, three limits of the Convention: first of all, the fact that, being a Treaty, it does not become automatically part of the domestic legal order of a MS; then, the fact that the ECtHR is not empowered to run a 'constitutional check' of the national legislation

security and liberty, carried out by Paul de Hert, underlines the hesitant attitude shown by the Court (at least until the *Marper* case, as discussed below) in recognizing some forms of data processing (as biometric techniques or other *soft* systems) as deserving the protection of privacy right *ex* Art 8 ECHR[276].

Moreover, it recalls to us that, assessing the 'necessity' of restrictive measures limiting some human rights, a margin of appreciation on the application of the Convention is left to the Member States. Therefore, not only different conventional rights receive different treatment but the same right can be limited differently, given, for instance, the nature of the state activities concerned (such as the fight against terrorism): this may justify a 'less strict standard of scrutiny', i.e., more freedom for the States to assess (at least initially) whether or not it is *necessary* for a democratic society to impede the exercise of individual rights[277] .

All these aspects, and in particular the *timid* attitude of the Court, seem to be the reasons for the scepticism of some authors (like the de Hert) in the 'dynamic influence', which could emanates (and, in fact, with *Marper*-case seems to emanate) from Art 8 of the Convention.

Such a dynamic, expanding effect deriving from a practical and effective interpretation of the Convention have already allowed the ECtHR to bring under the umbrella of the Art 8 threats derived from new means of communications [278].

This expanding effect is, hence, particularly relevant (for policy makers, legislators, governments) when assessing the *necessity* of new technological measures - that are contemplated in the many post-09/11 strategies – and would enable the judges of Strasbourg to use this protection tool also and (more importantly) in respect of new advanced technologies, even when apparently they are justified by security considerations.

Some techniques, unimaginable when the Convention has been written, started to be deployed in security contexts (such as airports, borders) and are

---

and that the applicant must demonstrate the detriment derived to him from the application of the law; finally he mentions the subsidiary nature of the protection provided by the Convention towards the national systems, prescribing only the minimum standards.

[276] It is useful to remember that limitations to privacy are justified, under the ECHR framework, not only if foreseen by the law and for a legitimate aim, and also if *necessary* in a democratic society; see Art 8 ECHR: (1)"Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

[277] De Hert (2005) *cit*., p. 73.

[278] See the telephone tapping case-law, Klass, Malone, in F. Sudre (2005), *cit*.; Van der Schyff, *cit*, p. 72.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

potentially damaging for privacy rights, especially if used in what one could call *AmI security (or detection) scenarios* (i.e., networked systems of AmI technologies used for security purposes).

In that context, data protection principles are not always applicable (e.g., because excluded expressively by the European directive, but also because it could happen that the AmI system's doesn't need to use *personal* data, in the sense explained above) and the assessment of their *necessity* in the name of security could be more difficult also due to a sort of *technological reverence* (measures are often considered necessary because technically effective).

This could easily result in unfair practices and unfair decisions about people who find even impossible (because unaware or because computer-illiterate) to contest these practices or decisions.

In a situation in which *soft* surveillance technologies are presented as indispensable to people, the criteria of *legality* and, especially, of *necessity* (*ex* Art 8, 2) need to be reconsidered in the light of the new human rights-related risks of these technologies: a 'legalistic approach'[279] should be replaced by a political, pragmatic one such as *constitutional reasonableness* and *subsidiary test* [280].

The hesitant attitude of the Court to recognize new threats deriving from new forms of data processing, seems to have its reasons, on one side, in the restricted concept of privacy (or better, of personal data worthy of protection) adopted, so far, by the Court of Strasbourg (not all personal data would fall within the scope of Art 8,1) and, on the other, in the interpretation of the *necessity* principle (art 8, 2).

Regarding the first aspect, although a prevalent inclination towards a broader concept of privacy[281], unsatisfactory criteria have been often adopted: one is that of *reasonable expectation of privacy*[282]. Hence, the Court has shown an excessive openness in recognising the existence of the legality requirement (Art 8,2) satisfied also in cases of unwritten law (*in specie* two cases law on wire-tapping), and justified by the phenomenon of continuous technological changes.

[279] D. P. Forsythe, *Human Rights Studies. On the dangers of legalistic assumptions*, Intersentia, p. 74.
[280] De Hert (2005), *cit*. p 81.
[281] See cases such as *Amann v. Switzerland* of 16.02.2000 and *Niemietz v. Germany* of 12.07.1991.
[282] According to De Hert this criterion seems "to invite to a Byzantium play of arguments about what privacy really is". The author provides the example of CCTV cameras, the reasonableness of which has discussed only in 2003, in *Peck v. U.K.* case of 28.01.2003. It has been already discussed in the first chapter on its dangerous effects. It can be added here that this criterion seems to increase the fear of a gradual erosion of privacy, the expectation of which is considered less and less 'reasonable', in relation to the rapid development of the techonology and to the gradual acceptance of new technology by people.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Against this substantive understanding of the 'law', that dangerously could foster acceptance, in an excess of discretion, of unwritten law as a legal ground for human rights limitation operated by new security enforcement technologies, a more formal approach to the legality requirement is recommended: as an expression of 'constitutional wisdom' ('no technology without law'), it would strengthen the HR framework in the field of criminal law[283].

Concerning the second aspect provided by Art 8(2) Convention, limitations to privacy should not only be foreseen by law, but also *necessary* in a democratic society. In other words, assessing a restrictive measure as lawful is insufficient, since the law itself could be 'unreasonable' and needs to be integrated by other criteria that reflect the basic values of a democratic society. For that reasons the necessary criterion has an extremely relevant role in the assessment of new possible security measures[284].

Art 8 (2) Convention provides for this criterion, but it appears that the ECtHR so far (at least until the *Marper case*, see below), has focused excessively only on the first criterion of art 8 (2), i.e. the legality of the interference[285]. The necessity requirement require consideration of the possible affected rights while balancing other (opposite) interests such as public security. The attitude of the Court appeared to be quite reluctant, i.e., often the Court even avoids the application of the second paragraph of art 8(2). The consequence is that cases of possible violation of privacy-related rights, through surveillance methods of public authority, have been considered simply not falling under the scope of Art 8, on the basis, for example, of the 'subjective' criterion of 'expectation of privacy'[286].

5.1. Soft surveillance technologies anchored to HR

If the requirement of necessity *ex* Art 8, 2 Conv. requires careful deliberations, it is, however, not difficult to recognize an unfair (and excessively loose) balancing among the individual's interests in enjoying a right and the interests

[283] See De Hert (2005), *cit.*, p. 78, who also points out the fact that the Court of Strasbourg, in several cases related to new investigation techniques, acted itself, as European legislator, remedying to the lack of legislative framework and providing MS legislators with a set of requirements (in particular foreseebility of the measures and of the conditions for their application), able, once met, to legitimate any measure privacy-infringing.
[284] See above EPIC about the new body scanners, *infra.*
[285] This requirement can be satisfied when the interference in private life has a basis in a law that is clearly foreseeable, accessible and providing remedies for the citizen without weighing thoroughly the other criterion, the necessity of a measure.
[286] De Hert (2005), *cit*. p. 80.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

of society as a whole in maintaining a restriction. Better, according to De Hert, to apply what he calls the criterion of 'constitutional reasonableness'[287], that would take into account the main scope of Art 8 Conv, i.e. avoiding unjustified concentration of power: a criterion that should be political, pragmatic and subject to revision, in order to be able to embrace new forms of surveillance measures[288] and adequately to address the dilemma between protection of society and respect of human rights (see below).

The scepticism towards a strong European HR framework showed by scholars as De Hert[289] seems based on the previous 'benevolent' assessments by the Court to *soft* forms of surveillance, characterized by a less strict scrutiny (i.e., a more margin of appreciation for the Member State) [290].

It must be noted that, in the assessment of the new surveillance measures as privacy-infringing ones, their technological features have an important weight, as they have in the application of the requirements of Art 8(2) (*necessity* in a democratic society). Observing the recent events and debates, it is possible to argue with de Hert that, in the majority of cases, the 'softness' of new surveillance measures (e.g., body scanners, biometrics and we can assume complex AmI security systems) and their (supposed) technological reliability "contributes to their legal receptiveness and to the apparently silence civil liberty arguments" [291].

In other words, new high-tech identification systems are often introduced with the argument that, without resorting to invasive physical contact, they can ensure more precise identification and authentication, disregarding that they treat, consequently, all citizens as crime suspects; that can be more privacy-invasive[292].

---

[287] *Ibid*. p. 84.

[288] Including those so refined that they appear soft, and apparently less damaging or invasive as well as those which are technically advanced so as to give the illusion of trustworthiness and accountability, while (being the first objective to be tricked by criminals, or because of negligence of police bodies) can produce dangerous false positive.

[289] It will be discussed later in the text how the second paragraph of art 8 Conv. and, in particular, the necessity principle has been rethought by the Strasbourg Court in recent judgments like the Marper case, which seems to have converted the scepticism of authors, like De Hert, into hope in respect of the efficiency of the HR protection instruments: see D. De Beer, P. De hert *et al*. (2010), Nouveax Eclairages de la notion de "donnés personnelle" e application audacieuse du critère de proportionnalité, *Revue Trimestrielle droits de l'homme* (81/2010), Bruylant, Bruxelles.

[290] Like wire tapping or other new control technologies, in which, as emphasised by De Hert, it seems more difficult to recognize a breach of fundamental rights simply because in place of the blood we find refined technology.

[291] De Hert (2005), *cit*. p. 90.

[292] See the debate on the possibility for the UK police to take and keep indefinitely, even from people not charged of any offence, DNA samples under the UK Police and Criminal Evidence Act (PACE), quoted by R. Brownsword (2008) Knowing me, Knowing you- Profiling and the public interest in M. Hildebrandt, S. Gutwirth (ed.) cit. In the following decision by the ECHR in the Marper case, instead,

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

As said before, the ECtHR limited its assessment of the necessity of security measures in a democratic society (Art 8, 2 Conv.) to a weak check of proportionality of security measures (to the legitimate aim pursued).

In the context of new technologies that can impact the HR protection, the subsidiary criterion would appear more useful: a technological invasive measure should be adopted when other less invasive measures, able to ensure the security interest at stake, are not available (*extrema ratio*). So far, this criterion has been rarely used by the Court of Strasbourg[293]; it must be noticed, nevertheless, that it calls for assessment of issues such as the concept of *invasive*, or *alternative*[294].

It can be argued that the subsidiarity criterion, complementary to that of 'constitutional reasonableness' could foster more resolute protection of privacy-related rights, but only if anchored to a human rights perspectives, instead of a technological one. Apparently biometrics seems less invasive but they are more dangerous from a human rights point of view (as indicated by the Court in *Marper* case).

The necessity principle requires a critical assessment and strict scrutiny of new technological measures (included *soft* surveillance devices) that, until *Marper* case, didn't seem to be adopted by the Court. Hence, it is a task for the European legislator to grasp the constitutional meaning of the HR framework to avoid the negative implications of the surveillance systems.

5.2. The *Marper* case (or…the careful consideration of the *necessity* principle)

In the discourse on the protection guaranteed by the ECtHR to the right of privacy, in light of the advance of new technologies used for security reasons, the S. and Marper case has been welcomed by scholars with favour, and even considered revolutionary in the context of the jurisprudence of the ECtHR on Art 8 Conv.[295]. Given the relevance of this case for the theme of emerging technologies used for security aims that impact HR, it deserves to be briefly recalled here[296].

---

the law itself (precisely the PACE) has been considered contrary to the standards of a democratic society (where, finally, a 'polical control' of HR infringements has been carried out).

[293] Except for the Peck case, as quoted by P. De Hert, *cit.* p. 93.

[294] De Hert (2005), *cit*. p. 94.

[295] R. Bellanova and P. de Hert (2010), Le cas S. et Marper et les données personnelles, *Cultures et conflicts*, n. 76, Harmattan, p. 101.

[296] The Court's view seems to be close to that of scholars (V. Andronikou *et al. Biometric profiling: opportunites and risks,* in Hindebrandt, cit.. p. 131), who have been lamenting in the last years the

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

It locates in the broader discussion on the the new security systems, that rely more and more on Information Technologies for the prevention and control of possible crimes, the form and the nature of which are, in this case, put in doubt by the ECtHR.

Surveillance is not only broader, deeper, disseminated in space but seems also 'dilutted' in time, since personal data (often sensitive) are collected, matched and stored in case 'it could be useful'. Before considering how this aspect has been at the centre of the *Marper* case and why it has been considered a violation of Art 8 Conv., it must be put emphasis on two aspects of these technologies, which re-bring us to the features of AmI: in many cases we deal with "smart" technologies, so-called because they work with a high level of automation, able to process large databases profiles through *ad hoc* software enabling the creation of precise criminal profiles for an efficient investigative action[297]. Furthermore, as previously observed, these technologies create the impression of "soft surveillance"[298], since they are apparently less intrusive and invisible. The invisibility is seen as less dangerous for private and social life[299].

---

risks to privacy and other rights deriving from the use of biometrics (especially when linked to profiles). Some of them, like iris, DNA and fingerprints contain medical information, so that a profile can contain prognostics on eventual diseases. Discrimination issues are at stake then when decision-making regarding a person is based on profiles related to her past activites, political, religious, ethinical or medical records. Risks of data-matching can be due to unauthorized access to some data or unnecessary collection of them. A person could be denied to access to some areas, or services, the latter "being prioritised according to extracted privileged group of people", candidates for job excluded on the basis of their medical or criminal records and so on. See also the criticism of the creation of the Italian national DNA Database (Law. 85 of 30 June 2009) in Andrea Monti, *Italian DNA Database: the devil is in the details,* EDRI-gram n.7.16, 26/08/2009, alleging the ambiguity of the law in the wording and in the technical references: in particular the law seems to lack any general obligation for the responsible parties to adopt serious security measures against unauthorized access or data tampering (with implications also for the right of defence, since an improper management of the chain of custody (as in computer forensics) should affect the admissibility of the evidence in Court – especially, given the recent findings that DNA samples can be faked without expensive means (http://www.scientificamerican.com/blog/post.cfm?id=lab-creates-fake-dna-evidence-2009-08-18);
any prior authorisation from a judicial authority to access the database is neither provided. Interesting also what the Monti says about the 'vicious loop' effect that could derive from the use of the DNA database in assessing crime impact: "crime statistics are based upon prosecutory investigations and trials, but if investigations are based upon the NDNA database, the only crimes that will be scrutinized by politicians will be those that fall into the database"; excluding 'white collar' crimes profiles from database, the potential result is an "injection of hidden racism".

[297] R. Bellanova and P de Hert (2010), *cit*. p.16.

[298] GT Marx (2006), Soft Surveillance, The Growth of Mandatory Volunteerism in Collecting Personal Information, in Monahan T. *Surveillance and Security. Technological Politics and Power in everyday life*, New York/London, Routledge.

[299] A. Rouvroy (2009), *cit*.p. 192, observes: "l'une des caractéristiques de ces dispositifs est justement leur relative invisibilité, leur naturalité[…] Que ces dispositifs fonctionnent effectivement, que la validité des predictions soient ou non démonstrées ne change pas grand-chose à la question de leur incidence normative".

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

It is in this context that we find the *Marper* case[300]. The applicants, two U.K. citizens (one minor) saw recognized by the ECtHR their right to privacy *ex* Art 8 ECHR against the practice of unlimited storage of biometric data (fingerprints, DNA samples and cellular profiles) collected from suspects of any kind of infraction) in the database of the national police. This occurred although the applicants had been acquitted or never brought to the Court. Their query of erasure of these (sensitive) data has been rejected by the police authorities, on the basis of the Police and Criminal Evidence Act (PACE) of 1984.

Once it had acknowledged the infringement of Art 8 (1), the Court devoted itself to the issue of the possible justification of this infringement, deriving from the respect of the three requirements indicated in Art 8(2) (i.e., limitation provided by the law, for a legitimate aim and necessary in a democratic society). The legal basis and the legitimate aim (prevention of crimes) were satisfied according to the Court (although the British law was considered vague so that it should have raised doubts in the U.K. whether the measures were prescribed by the law [301]). It was not the same for the third condition, the *necessity* in a democratic society: the Court focused, as it hasn't done before, on this aspect, that should imply a balancing activity to establish which rights/interests are predominant, even if it reduces this analysis to the verification of the proportionality test.

The innovative approach of the Court is testified not only in the recognition of unlimited storage of biometrics from not-convicted persons as in breach of Art 8 ECHR, but also in the reasoning given, that attempt to limit the 'simple storage', considered *per se* as stigmatizing, especially if one consideres the technologies used[302].

The relevant conclusion of the Court, that acquires a general meaning for the assessment of new technological security measures, (thus, also for *AmI security scenarios*), is that the unlimited storage of sensitive data such as biometrics cannot be considered "necessary in a democratic society", as required by Art 8(2): the criteria indicated by this article, infact, should be satisfied all together in order to make it applicable (i.e., to allow limitations to the right to privacy) and the Court has found that it was not the case in the Marper judgment. On the contrary, the British government claimed the need for the storage of biometrics for prevention and

[300] ECHR *S. and Marper v. U.K.* of the 4 December 2008.
[301] D. De Beer, P. De Hert, G. Gonzalez Fuster, S. Gutwirth (2010) Nouveax Eclairages de la notion de "donnés personnelle" e application audacieuse du critère de proportionnalité*, Rev. Trim. dr. h.* (81/2010).
[302] R. Bellanova & P. De Hert (2010) *cit*. p. 18.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

detection reasons (§ 94) in particular, for the inestimable value of the material stored in the fight against terrorism, allowing the identification of people in a way that was impossible before[303].

The importance of the Marper judgment could be found, first of all, in the 'integrated' protection that the Court grants to personal data; as said above, the ECHR contemplates explicitly only the right to private life, that, though traditionally extended by the jurisprudence of the Court to personal data[304], it cannot be considered coincident: personal data-processing will be protected under Art 8 ECHR if that is considered pertinent on the basis of the nature of the data, of the processing and of the context. The enlargement of the definition of personal data worthy of protection, because playing a fundamental role in the exercise of the right to privacy, that the Court operates is, thus, meaningful[305] and permits hope in respect of the protection of biometric data processed in an AmI world.

The other reason that makes this decision revolutionary is the attention for the criterion of "necessity in a democratic society", that is intimately linked to the concept of 'proportionality' (§ 101)[306]: an approach that have been previously avoided by the Court, more focused on formal criteria such as that of legality[307].

The Court recognizes that the generalized storage of biometrics from suspected but not convicted persons creates a noteworthy power (§125) and that this does instantiate an unacceptable *equilibrium* among the public and private interests at stake: this storage would be not proportionate with the applicants' rights[308].

Before the *Marper* case, as properly observed [309], the jurisprudence of the ECtHR gave us little reason for optimism about the safeguards offered by data

[303] Even though it is not directly mentioned in the Marper case, this claim of the British government gives occasion to think about the issue of the reliability and efficiency of new technological measures as a value *per se*: every new technology would be justifiable according to the sustainers of this view since it would allow for advantages (precision, reliability, affordability) previously unimaginable (see below).

[304] See F. Sudre, *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005.

[305] R. Bellanova & P. De Hert (2010), *cit*. p. 19, who find corroboration of this approach also in Bouchacourt c. France, 17 December 2009.

[306] De Beer et al.*cit*. p. 156.

[307] It is interesting also the comparative analysis made by the Court, on the basis of which it justifies the reduced margin of appreciation of which a state - in the case, the U.K. - could dispose in order to decide of the limitations to privacy right – due to the strong *consensus* that exist in the other Member States about the unlimited storage of biometric data, although, as stressed by de Beer *et al. cit*., p 159, this approach could also be dangerous: the Court would have decided differently if the majority of the states was in favour of the unlimited storage?

[308]Recognizing that the "simple storage" of personal data is a risky activity *per se,* the Court seems to uphold the orientation of the main European doctrine (as mentioned earlier) and of the Art 29 Working Party, the independent European advisory body on Data Protection and privacy.

[309] De Hert (2005), *cit*. p. 93.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

protection and privacy, especially in respect of the use of new technologies for security purposes: a claim would have been possible only in case of concrete misuse or abuse of the databases by the law enforcement authorities, i.e. when it was possible to establish that this use would have had negative consequences for the individual (but how to demonstrate it without knowing even the existence or the logic?)[310].

In *Marper* case the Court considered that even the 'simple' storage of data represents an interference into private life, independently by the following use that could be done of them, allowing in this way to extend the protecting cover of Art 8 ECHR also to data processed by new security measures that apparently limit themselves to the 'mere' storage of personal data (as said about some detection technologies).

5.3. Implications of new surveillance practices on other rights and the relevance of privacy protection

The *Marper* case is linked to the general debate on the current adoption by the society of new surveillance practices (such as the automated, smart, detection technologies) and to the role that the right to privacy (could) play towards these practices also in support of other rights.[311]

It must be noted that some rights of defence, in particular the principles of innocence and the rights not to self-incriminate (*nemo tenetur*), in many cases invoked in the debates against the surveillance techniques and formally recognized by the ECHR (Art 6), are declared not always evocable: due to its procedural nature, Art 6 is subject to limitations (can apply only to persons accused of any infraction and this infraction should be of criminal nature)[312]. It means that the formal acknowledgment of these rights can do nothing against the use of *smart and soft*

[310] As observed by Bellanova & De Hert (2010), *cit*. p. 19, the change is appreciable, especially if precedent is are taken into account. In the case of *Friedl v. Austria*, of 31/01/1995, (photographing of a participant in a demonstration and recording of information concerning him) the Court- *rectius* the Commission- arrived at the opposite conclusion: the simple storage of personal data by the police could be considered *necessary* in a democratic society whatever there is any 'critical' use of them (i.e. abuse or misuse of them); in Marper, instead, it does not matter if a critical use has been done or not. In another important decision, the *case Leander v. Sweden* of 26.03.1987, the Court have recognised that the storage of data in the secret files of the police would have been an interference in private life, *ex* Art 8 of ECHR, but that this practice was justified by the presence of the three criteria required by Art 8 (2).

[311] See D.J. Steinbock (2005) *Data Matching, data mining*, Georgia Law Review, vol. 40, 1, who stresses that, these technologies for their functioning based on collection, storage and profiling analysis, would increasily engendera culture of suspicion.

[312] See Bellanova and De Hert (2010), *cit*. p. 23.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

technologies of modern surveillance, since apparently with their use there is any right to the silence to be respected or any subject accused of any infraction.

Here the right to privacy could show its potential as instrument for the protection of other rights: as explained above, the Court, regardless of the possible further use of the data, recognized the implicit risk of stigmatization of an innocent deriving from unlimited storage of his/her data (potentially enabling discovery of the genetic relationship of the person)[313]. The Court, in this way, shows to search for a good *equilibrium* also with regard to the values underlying the presumption of innocence (Art 6), while it discusses about the necessity of biometrics storage; though recognizing the usefulness of databases for crimes-detection scopes, it highlights the risks of stigmatization deriving from certain security procedures, meant as risk of making the category of 'sospect' perpetual[314].

It is worth noting the reflection made by the Court about the fact that the ethnic identity (that could be revealed by the data analysis) of a person should be considered as an important element of private life to be protected: privacy as an instrument against discrimination. This aspect is likely to have a special relevance in the context of new technologies, not only due to their increasing profiling capabilities but especially because the deployment of *biometric profiling* techniques (see *supra*)[315].

In this way the Court clearly broadened the field of application of Art 8 Conv., including also a social nature of the right and confirming a trend towards the integration in the field of application of Art 8 ECHR of the protection provided by the Conv n.108/81, considering the storage itself as interference in private life[316].

As stressed by De Beer *et al.*, in the context of criminal and security policies, the former III pillar of the European Union, the Member States have a greater margin

[313] Although the Court's reasoning in *Marper* case, taking into account the following processing to which the different data could be subject (systematic storage in data bases, use for criminal identification etc.) seems to keep some ambiguity as for those cases in which data are not yet used (as claimed by de Beer *et al. cit.*, p. 155), it does not seem, nevertheless, a contradiction; the Court considers the eventual processing (not yet operated) as the possible 'danger' to individuals' rights.

[314] The Court tried to limit these practices, pointing out that the unlimited storage of data would sanction in disproportionate way individuals that belong to the category of innocents, linking them, unjustly, to the *status* of criminals (§122).

[315] This might cause one to reflect on the international law policies on migrants and the security measures taken especially at the borders, where new technologies, aiming at detecting and identifying criminals suspects and including facial recognition techniques (often real-time and interconnected with criminal databases) are being introduced (see *supra*).

[316] This interference as regards people acquitted or simply 'ex-suspects' is not justifiable, according to the Court (because unnecessary in a democratic society): thus, what would have been the attitude of the Court if the applicants had not been acquitted? Probably, the considerations on the storage of data as invasive would have not been the same.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

of appreciation -in particular when there is not a *consensus* on a certain matter[317]. In this context, the Court has showed itself prudent, limiting its assessment to evaluate the existence of this *consensus* (little *consensus*, greater margin of appreciation), and the compliance of security measures with the national law (taken by the States in their large discretion in criminal matter): it seems that the Court had mostly preferred to avoid the slipping field of security enforcement, and, thus, to analyse the more 'political issue' of the necessity in a democratic society, that would have brought more often to oppose state (invasive) measures taken in this area[318]. In particular a general absence of application of the subsidiarity principle there has been noted, that would have led to a consideration of the different available alternative measures[319].

For that reason, the *Marper* case is innovative. More importantly, the application of the necessity principle is not excluded simply by the efficacy of these techniques in preventing criminal offences[320].

Rightly, this judgment is considered as generator of new life for the principle of '*necessity* in a democratic society'[321], with which the limitations to the right to privacy– especially if through surveillance technologies - must comply.

Recently, the German Constitutional Court adopted an innovative judgment on the proportionality requirement when informational privacy is at stake[322]. The occasion was offered to the Court by the German law implementing the Data Retention Directive[323]. The Court suspended the law because it breached the constitutional requirement of proportionality. Proportionality of the national law (not unconstitutional in itself), according to the German Court, means respect for purpose

[317] It is likely that the situation will change with the recent entry into force of the Lisbon Treaty (see below).

[318] It must be recalled here that Member States "have a positive duty to take reasonable and appropriate measures to secure the applicants' rights under Art 8 and to strike a fair balance between the competing interests of the individual and of the community as a whole"; see ECHR *Hatton et al. vs U.K.* 02.10.2001. See also G. Van Der Schiff, *cit* p. 66.

[319] See De Beer et al. *cit*. p.156, who quote rare cases (such as *the Hatton et al*. case) in which this is done.

[320] Two passages of the judgment are particularly interesting here: (§. 112-118) that one in which the Court declares unacceptable a weakening in the protection offered by Art 8 that would occur in case of admission of modern technologies in the criminal system at any price and without a due consideration of the essential privacy-related interests. Furthermore, the Court stresses that a State affirming to be a pioneer in the development of new technologies bears the responsibility to find the *equilibrium*.

[321] De Beer *et al., cit*., p. 160.

[322]German Constitutional Court, Judgment of the 02/03/2010 available at http://www.bverfg.de/en/press/bvg10-011en.html, which follows to at least other two meaningful decisions of the same Court affirming the 'informational self-determination' in1983 and the right to 'computer confidentiality' in 2008.

[323] The 'Data Retention' Directive 2006/24/EC had been declared by the ECJ (Judgment in Case C-301/06 *Ireland v Parliament and Council* of the 10/02/2009) to have an appropriate legal basis in the ex art 95 of the TEC.

limitation, data security, transparency and control against misuse[324]. The judgement is particularly relevant because it extends the protection of communication to the location and traffic data (circumstances of communications) that could reveal also sensitive data and could allow the creation of behavioural profiles at the (direct or indirect) use by law enforcement authorities.

6.'Controlling' technologies. Smart technologies and the new risks of stigmatization

With the *Marper* case, as explained above, the risks of stigmatization seem, though in an indirect way, to find a judicial answer: the judgment offers the instruments to limit the impact on people's basic rights of *smart and soft* technologies, even when the latter operate in *stand-by* mode, as in the case of 'simple' storage of data[325].

In particular, since these technologies are used increasingly (also) by the public authorities, for observation, identification, prevention as instruments of the (general) activities of government (so for security aims and otherwise), some scholars considered them as the undisturbed symptom of such a transformation in the logics, strategies and tactics of governments to bring about a gradual conversion of the traditional government into a "*statistic government*"[326]. Paraphrasing Foucault, the main aim of governments in the profiling age would be *detecting and preventing*.

It might be not so odd to call our times a 'prevention age' if one observes all the detecting and pre-emptive practices put in place by governments, in the aftermath of 9/11[327]: some of them showing even a sort of anticipation (not only of the judicial process but) also of the punishment, as well as to recognize a dangerous trend to punish even the mere intention of people (against the basic rules of criminal law in a democratic society).

[324] In this way, the German Court adopted a privacy test similar to that developed by the ECHR, see *Goodbye Unlimited surveillance, Hallo proportionality*, by P. De Hert, R. Bellanova, K. de Vries available at http://vortex.uvt.nl/TILTblog/?p=118 and K. de Vries, R. Bellanova & P. De Hert, Proportionality overrides unlimited surveillance, CEPS, Liberty and Security in Europe/May 2010 http://www.vub.ac.be/LSTS/pub/Dehert/342.pdf.

[325] R. Bellanova & De Hert (2010), *cit*. p. 27.

[326] A. Rouvroy (2009) cit. p. 248.

[327] See the examples of detection technologies given before.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

With regard to investigative measures (and detection technologies) it is possible even to observe certain failures of the justice system, when these measures result in unjustified stigmatization, lack of due process, wrongful suspects/arrest[328].

The main idea underlying the concept of 'statistic government' (*supra*) is that the governmental action, in order to manage uncertainty (regarding either the private consumption or the criminal acts) needs to test the present in order that it could reveal its potentiality and could facilitate the anticipation of facts, actions, even intentions. Here it is that an 'efficient' answer is offered by the new smart technologies (such as those described in the AmI scenarios). These systems, as explained above, combine a set of sensors, disseminated in the environment in order to collect data on persons, behaviour or events, and store them in computers, which, through special profiling algorithms and statistic correlations, can interpret the data according criteria of normality or abnormality and, afterwards, automatically to adapt to the situation or to signal it (e.g. as abnormal).

The "*gouvernance statistique*"[329] would aim at the prediction of and at the pre-emption of the behaviour of the individuals (that could be, in this way, better 'subdued')[330].

Worth mentioning, as they impose further reflections on surveillance detection technologies, are the tacit assumptions on which the logics of the *statistic government* would ground: first of all, 'the body does not lie' idea, according to which the detection devices and systems would find in the physical body itself a privileged source of predictive information, to the detriment of elements of the economic, social, cultural context of the subject: the personal declarations, hence, lose any value in front of what algorithms of the statistic correlations say[331].

[328] Report of the UN Special Rapporteur (2009), *cit*. p. 13.
[329] On the notion of *governement statistique*, A. Rouvory & T. Berns (2009), *Détecter et prévenir: de la digitalisation des corps et de la docilité des normes*, in L. Guy - J. Mariau (eds*.) Gouverner par les corps*, P.I.E. Peter Lang, (forthcoming).
[330] See A. Rouvroy (2009), *cit*. p. 192, who stresses the impact of these practices on the life of the subjects, the civic, political, economical or social existence of which appears to be fragmented, de-contextualized and, finally, manipulated according to the contingent finalities.
One could find an echo of this analysis in the article of the Italian journalist G. Bocca, "Intelligence double face", L'espresso, 22/07/2010, in which he wonders about the real function of the so-called 'intelligences' and finds two main concrete scopes: they are useful for the good affairs of the state leaders (*buoni affari dei padroni degli stati*) and to keep up the presence of facing the societal chaos, that is, to justify the use of the intelligence by the governments with which they dominate the chaos".
[331] A. Rouvroy, Detecter et prevenir, *cit*. p. 3.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Another assumption is that, once the collection of a huge amount of data is ensured to which to apply the algorithms, everything can be prevented, without the need to know causes and deeper reasons[332].

From a legal point of view, what matters more is probably the fact that the subjects do not have the possibility to contest and impugn the validity of these profiling activities or of the predictions made on their account, since they even do not know about the existence of these statistic practices or they do not understand their functioning, nor they can challenge the decisions eventually taken on the basis of the algorithmic results. This normalization of behaviour is inevitably linked with the exercise not only of right to privacy (*strictu sensu*) but with the right to defence (and in particular with the due process, *ex* Art 6 ECHR) [333].

In the Rouvroy's opinion, the main threats would reside, therefore, in placing the elaboration processes of the norms (also made by technologies) outside of public debate, in its de-politicising, as well as in the lack of a judicial assessment about the impact of the algorithmic profiles on the enjoyment of certain fundamental rights[334].

6.1. The value of Self-determination in new technological contexts

An important aspect described by the privacy concept, that seems to be particularly suitable in the assessment of the new (surveillance technologies) is the tension between individuals and community[335].

A refined concept of privacy seems therefore desirable and derives from the need to keep its main role as a right also in the contemporary technological world: protect fundamental values of democratic constitutional states, guarantee individuals' freedom of self-determination, their right to be different, their autonomy in

[332] A. Rouvroy, *ibid,* writes: "[Les sujets] en fonction du contexte, seront, alternativement, virtuellement ou potentiellement criminels, consommateurs, employés zelés ou démotivés, sans possibilité de repositionnement de ces fragments éparts en fonction d'un fil autobiographique".

[333] *Ibid*. The author argues that if the codes become the 'norms', it would be almost impossible for the subject, who is identified by the statistic correlations as 'deviant', to explain the (contingent, personal) reasons for which she departed from a certain behaviour. This seems to corroborate the claim made by M. Hildebrandt about the need for an Ambient Law and for literacy in new technologies (see *infra*).

[334] In this way, Rouvroy seems to embrace a more radical approach than Hildebrandt does, arguing that it would be insufficient to consider the new technologies under the perspective of threats for privacy and data protection, but it would be necessary to consider the new devices in respect of the new ways knowledge is produced (as well as the effects for the governments and for the public process that come from this knowledge).

[335] M. Friedewald, D. Wright, S. Gutwirth, E. Mordini, Privacy, data protection and emerging sciences and technologies: towards a common framework, *The European Journal of Social Science Research*, vol. 23, n.1, 2010. p. 61.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

relationships, their freedom of choice as regard social behaviour, health, sexuality etc.[336].

The new ways of construction of digital memory, its increasing capacity and different uses bring some scholars to question whether it is possible to 're-invent the art of forgetting' in the Information Society, or rather in the knowledge society[337]. The new forms of knowledge-creation passing through the current technologies transform, in fact, the process for the free development of the individual personality, an issue of legal relevance, given that central role self-determination has within the data protection regime[338]. It is necessary, therefore to rethink the ways the subject could keep this prerogative, in spite of the intensification of surveillance, profiling and traces of her movements, choices and emotions. The reason for the protection of individual self-determination lies, infact, in being one of the necessary conditions for the individual autonomy in a democratic society: i.e., to have the possibility to change opinions, ideas, behaviours, to explore new ways of life without being considered as 'deviant'[339].

As Rouvroy argues, it is the right to 'a second occasion', not to be reserved only to those who have already served a punishment, but to be protected for the whole population: while this *droit à l'oubli*[340], imposes already in a democratic society the duty to erase after a certain time the reference of a conviction from the court records, governments strategies (like the P.A.C.E. in U.K.) and biometric industry seem going in the opposite direction (and with regard to the data of all citizen)[341].

---

[336] M. Friedewald *et al. cit*; De Hert, S. Gutwirth (2006) Privacy, Data Protection and law enforcement. Opacity of the individual and transparency of power, in E. Claes, *et al*. *Privacy and the criminal law*, Antwerp, Intersentia.

[337] A. Rouvroy, Réinventer l'art d'oublier et de se faire oublier dans la seciété de l'information? In S. Lacour (Ed.), *La sécurité de l'individue numerisé*, Paris, L'Harmattan, 2008, p. 249-278.

[338] The aspect of individual self-determination could apparenty refer only to the private sphere of data protection and privacy rights, though it expresses itself often in the public and social dimension (autonomy and freedom of interferences in decisions regarding politic, religion, philosophy); but the intensification of surveillance practices in the different sectors of society, public and private, blurring the purposes for which personal data are used, creating *ad hoc* profiles from different databases, coul blur the outputs of these practices. The limitation of the individual self-determination could turn into impact other fundamental rights, such as free movement, freedom of expression, physical freedom: deviant behaviour (for political, social or commercial statistics, can be matched with criminal databases, becoming automatically a typical (profiled) 'criminal deviant behaviour'.

[339] These reflections might bring to see the dangers in the behaviour-detection technologies (like some of those introduced by the Israel government that, we can presume, will not be limited in the next future to security field.

[340] See the recent consideration of the BEUC (European Consumers' Organization) about the right to be forgotten in the digital age available at http://ec.europa.eu/home-affairs/news/consulting_public/0003/contributions/registered_organisations/beuc_en.pdf.

[341] As showed by many of the emerging techologies described in Detecter, Survey n 3,4,5 and mentioned *supra*; it is an interesting example also the recent system – a sort of black list of bad

With technological developments[342], some scholars have even suggested to come back to the original concept of privacy, the right to be let alone, deemed as implying the relationship between citizen and government[343].

As noted in the first chapter *infra*, AmI technologies and pervasive computing can impact the individual's life, changing his/her habits, and manner of relating to the environment: sensors, Rfid tags, cameras or other advanced devices can track items and persons' movements to collect, interpret, match and re-alaborate data in real-time in order to promptly provide individuals with suggestions or other information services.

In the scenarios imagined in computer science many of these reasoning and informative capabilities of the pervasive computing are presented as an innovative way to amplify and facilitate individual choice: the system will offer a range of possible solutions (roads, stores, items to buy), but you 'choose' the one with the best rate.

The limitation to freedom of choice is one of the main issues at stake when considering the impact on privacy by AmI technologies (beside the fact that tracking movements in a pervasive computing environment is considered already as invasion of user's privacy, since the system is always aware of the user' location and activities). Since everything in an AmI world tends to be automated and real-time, the choice of individuals tends in parallel to be reduced, even when apparently the system leaves the last word to the user: he will decide among packaged possibilities, suggested on the basis of his (supposed) preferences and profiles, without having the occasion to change tastes and opinions[344].

One of the alarming effects of those surveillance measures, that have as objects the web preferences and communications among Internet users – especially if politically dissident to their governments - is to generate in users the fear even to

---

guesses - adopted by many hotels and B&B in the U.K. http://www.guestscan.co.uk/what-is-guestscan.html; chilling effects seems to derive also from the new (at least for Italy) service offered by 'gmail', *Priority Mail*, which relies on the powerful algorithms of google to select and classify the mail that is (or supposed to be) a priority read: http://www.youtube.com/watch?v=NbSp069ZnUI.

[342] It must be noted that the same advocates of rights to privacy do not reject these technologies *tout court* but they advocate for them a refined framework. See D. Le metayer & A. Rouvroy (2008), *STIC et droit, conflits et complémentarités*, Interstices, ed. INRIA, available at http://interstices.info/jcms/c_34521/stic-et-droit-defis-conflits-et-complementarites.

[343] F. Sudre, *cit*. p. 25.

[344] A. Rouvroy (2008) *cit*. p. 248. The idea of Mark Weiser, pioneer of pervasive computing, speeking about natural interaction and comparing language in printed form (we do not notice that information is being transmitted when we see streets signs) with pervasive computing, was that this will exist when it become so natural that people do not even realize they are using computers and technologies (for that reason devices will need to rely on global networks that emphasize wireless technologies, large databases and profiling capability); see http://www.ibiblio.org/cmc/mag/1995/apr/last.html.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

communicate, to visit websites or to express their opinion. This causes negative consequences[345].

The legitimate deterring aim with regard to criminal acts is transformed, in this way, into illegitimate deterrence with regard to democratic rights freely to express their opinions or dissent against their governments. In an AmI world these fears will be augmented, not only because of the 'Interent of the things' (see *infra*), but because of the fear to be continuously monitored, everywhere, in every moment.

Moreover, it has been observed that a trend already supported by IT companies such as Microsoft is to build giant centralized server all over the world to house their next generation of applications: that makes easy it to imagine how a relevant control power will be concentrated in these companies[346].

We still do not know how the world will look in a full AmI, "when everything becomes connected" [347] but, considering the possibility that all of the data from daily-life transactions or even from surveillance technologies are connected and used (improperly) by private organizations, the impact on privacy (and related rights) will be undoubted noteworthy [348]. The situation seems alarming if we put together these visions of AmI (therefore, not yet completely realized) with the already proved experience of data collection and exchange among government agencies and private companies[349].

New technologies are going to change many aspects of our private and social life, creating new contexts: even before the realization of a complex AmI systems, as imagined in some science-fiction movies, many of us already create in everyday life an own 'PAN,' personal area network, in which technology enables wearable computer devices to communicate with other computers and exchange data[350].

Differently from those which led the industrial revolution, new technologies, are less complex, lighter, decentred, disseminated and their control is mainly in the

[345] See A. Rouvroy (2008), *cit*. p. 249.
[346] See J. Ridges (2008) *cit*, p. 735: an example is given by MIT, with a Project called Oxygen (to give the idea that pervasive computing become like the air we breathe), a human-centered pervasive computing-like the air we breathe- that recognizes individual needs, activities and movements and then adapt consequently the environment, www.oxygen.lcs.mit/).
[347] J. Ridges (2008), *cit*. p. 725, who discusses the dangers of privacy deriving from interconnectivity and pervasive computing.
[348] 'Pervasive computing' is defined by the Centre for Pervasive Computing, www.pervasive.dk, as next generation computing environments with information and communication technology everywhere, for everyone, at all times", inspired probably to the Microsoft CEO Stave Ballmer's statement of 1999 on the future of computing as "anybody, anywhere, anytime, connected to Internet, on any device".
[349] De Hert (2005), *cit*, p. 87.
[350] See: http://windows.microsoft.com/it-IT/windows-vista/What-is-a-Bluetooth-personal-area-network-PAN.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

hands of individuals or small groups; as it has been observed by Friedewald *et al.* the challenges deriving from the emerging technologies result "in a growing gap between citizens, technology and politics, notably when the individual's private sphere conflicts with the notion of common good"[351].

This supports the need presented in the first chapter of privacy as a social good: the only possible dimension that can be balanced with other social interests such as security (or free speech). A social perspective of privacy appears, hence, particularly necessary especially with regard to detection technologies used for security aims.

As stressed by M. Friedewald *et al.,* considering privacy solely in individualistic terms has as consequence that privacy is undervalued: "protecting privacy of the individual seems extravagant when weighed against the interests of society as a whole"[352].

If privacy should also be seen as a social good, the public debate claimed by scholars such as Rouvroy and Gutwirth against the inherent de-politicization of the 'statistic practices', become even more urgent[353]. So far, the focus has been on legislation, but initiatives such as the EU's RFID consultation show an important change of direction, towards Privacy Impact Assessment (PIA)[354], defined as "the

[351] M. Friedewald *et al., cit*., p.63.
[352] *Ibid*. p. 65.
[353] An interesting example of mobilization of public opinion on effects of new technologies is offered by the initiative supported by the Belgian LigueDH: debates and protests of different nature have been organized in September 2010 against the replacement in Brussels of the traditional tickets for public transport with an obligatory smart card. As argued by Standeart, Rouvroy *et al.* in the article "*Carte MoBIB, un bon example de mauvaise mise en oevre*" (ww.liguedh.be), the specific system (that allows the automated processing of data stored in the card) is contestable for compliance issues with the privacy law; the critics aim not to oblige the responsible society to withdraw the card but to help it in being compliant with the law. It is claimed, first of all, that there is a lack of information ('an unnecessary opacity') regarding the security of the systems (that should be frely available to the users) and, secondly, that there is a failure to provide an alternative system to the user; moreover, it has been verified that personal data contained in the card cannot avoid to be easily 'read' by third parties; finally the system does not comply with the principle of proportionality with regard to its finalities: detecting the fraud and managing the traffic in the metro are scopes that can be sought with anonymous data, at least at the first stage, according to the principle of minimization. The authors, therefore, argue for an 'un-traceability by default', instead of a data use by default. The initiative shows, on the one hand, the danger of a badly controlled technological development, and, on the other, that a compliant technical solutions should be preferred, whatever is the cost of the compliance or the supplementary period of time needed before a generalist adoption of automated means become a reality.
[354] The consultation of the stakeholders on the development of a new technology such as Rfid and the recommendation of the use of privacy impact assessment in new applications is a recent tool in Europe; according to M. Friedewald *et al.,* its use is likely to grow in the next future. See the recent Art 29 WP *Opinion 5/2010, WP 175, on the Industry proposal for a privacy and data protection impact assessment framework for Rfid applications*, of the 13 July 2010, in which it is stated that the Working Party does not endorse the proposed framework in its current form (given "the absence of a clear and comprehensive privcy risk assessment approach"). See also Bennett *et al*. *Privacy impact*

systematic process for evaluating the potential effect on privacy of a project, initiative or proposed system or scheme" [355].

The importance of PIA can be seen, especially if correlated with the reflections on privacy problems of Solove (see I chapter, *infra*), since this instrument facilitates anticipation of at least the main consequences of the technologies (often new and undesirable) and therefore establish appropriate HR policies to minimize the negative effects.

6.2. The social dimension of privacy right(s)

As underlined above, the right to privacy has also been considered by scholars and by the Courts also as an instrument to guarantee respect for other rights (or without which other rights would not be effectively enjoyed) [356].

For this reason, it is important that privacy is considered in its social dimension (in addition to its individual dimension), as necessary for the enjoyment of rights such as due process, free movement, freedom of association, freedom of expression as well as for ensuring the decisional autonomy of individual[357] to develop opinions and make choices without unwanted and unaware conditioning or chilling effects.

In that context, some prerogatives, essential for the social life of individuals, have been identified as conditions for the enjoyment of rights and freedoms guaranteed by a democratic state: a sort of meta-rights (*droit à l'oubli, droit à la désobéissance, droit de (se) rendre compte*) that appear to be affected by the configuration of the possible field of action, at a 'pre-conscious' stage and through the use of suitable algorithms by the '*governement statistique*'[358].

As underlined by the UN Special Rapporteur in its Report A/HRC/13/37, surveillance techniques can affect these rights and freedoms often in combination. Another way in which surveillance mechanisms are eroding the right to privacy is in

---

assessment: international study of their application and effects report for the Information Commissioner's Office, London Linden Consulting, 2007 available at http://www.ico.gov.uk/ .

[355] R. Clarke (2009), Privacy Impact Assessment: its origin its development, *Computer Law and Security Review*, vol 25, 2.

[356] See the conclusions of the ECHR *Marper* case, *cit*.

[357] A. Rouvroy (2008), *cit*. p. 248.

[358] A. Rouvroy (2009), *cit*., p.189. In its recent judgment on data retention the German Constitutional Court (*supra*) seems to echo these considerations, holding that "a preventive general retention of all telecommunications traffic data[…]is to be considered as such as heavy infringement because it can evoke a sense of being watched permanently"; moreover it appreciates the fact that the data "are not at the State's disposal as a total collection", avoiding a "potentially blanket measure of preventive data retention" (§218).

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

the increasing data exchange agreements or policies among intelligence agencies that are kept secret and not publicly available for any objection and review.

This aspect matters especially if we think on the wider possibilities offered to the law enforcement agencies by new technologies that can rely on a network of ubiquitous computers connected to each other and to remote databases, through which group profiles can easily be created. Concerns are even more major if we think that the exchange of data and the cooperation in the fight against terrorism occurs not only among governments but also among these and private subjects, such as banks and telephone companies [359], which hold huge amount of personal data.
A dangerous merging of both public and private data and control activities has started to be perceived[360].

Some cases in the US demonstrated the dangerous argument of 'reasonable expectation of privacy' (see *supra* de Hert) (especially when a legal basis for the interference is not required) that, according to the American Supreme Court is narrowed when the data are 'freely' shared among these parties.

In EU, the increased calls for data collection and data storage, become binding with the Data Retention directives that have been criticized[361]. It is necessary to add another note. Data Retention measures have been introduced as exceptional measures, and, as other exceptional measures, should be taken for a limited period or time.

As affirmed by Weyembergh, "*La vulnérabilité des démocraties au terrorisme en raison meme de la liberté qu'elles rendent possible, ne doit pas les mener à des reactions excessives*"[362]. In particular, we can consider always valid, in the assessing the recent measures adopted (*in specie* the technological ones), the three conditions of Wilkinson for 'democratic answers to terrorisms' quoted by Weyembergh: all the measures and their application should remain under the control of the civil authorities; all the anti-terrorism measures should remain within the law; it is necessary to maintain the legal processes (*mantenir les proces légaux normaux*); the exceptional measures should be adopted by the legislator for limited period of

[359] Report of the Special Rapporteur, *cit*., p. 15.
[360] See M. Hildebrandt (2008), *cit*. p. 110
[361] The Special Rapporteur (Report *cit*. p. 20) is concerned that in many countries data retention measures have been adopted without any legal safeguards regarding the access to this information being established and that new technologies blur the difference between content and communications data.
[362] M. Weyembergh (2002), Le Problème, in E. Bribosia, A. Weyembergh, *Lutte au terrorisme et droits fondamentaux*, Bruxelles, Bruylant, p. 25.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

time; moreover they should be clearly formulated, made public and annulled when the circumstances change.

The consideration of Weyembergh also appears particularly useful for an analysis of high-technological answers to terrorism: if the 'total terrorism' appears to be no more than a threat, the conditions just mentioned must be respected: "*les démocraties doivent garder leur sang-froid et éviter les mesures anti-terrorists qui seraient contre-productives et mineraient les libertés démocratiques*"[363].

Regarding the measures against terrorism financing, advanced data-mining tools are used by financial institutions to access to people's transactinal data and in some cases the same institutions facilitate third Government access to their databases to find terrorist suspects, although this practice result to be in breach of many national privacy law (as testified by the SWIFT network)[364]. It could be said that the attempt to combat money laundering risks encouraging data-laundering.

In order to avoid abuse due to the vulnerabilities and implicit risks of the surveillance technologies (unauthorized access), a stronger system of liability should be developed and special sanctions should be established for those who access data without being entitled or who abuse of their privileged access. Therefore, it is essential that at the technical level the surveillance activities could themselves be monitored through log files that allow to know precisely who accesses the data.

7. Challenges and opportunities under the Lisbon Treaty. Concluding remarks

One first conclusion can be drawn on the basis of the observations collected: the security trends observed above as reactions to 9/11 attacks, initially limited and provisional, brought to an extension of the surveillance powers beyond the fighting against terrorism: what was before exceptional became customary[365]. Reviews of legislation and special strategies have been introduced in many countries and extraordinary powers have been given to law enforcement agencies to conduct investigations not necessarily related to terrorism[366].

[363] *Ibid*. p. 32.
[364] See http://www.personuvernd.is/media/frettir//pr_11_10_07_en.pdf.
[365] Report of the Special Rapporteur, *cit*. p.17-20.
[366] Some of them can be briefly recalled here: The UN Security Council Resolution 1373 (2001) on terrorist-listing; the EU Council Counter-terrorism Strategy of 2005 ("*Prevent,Protect, Pursue, Respond')*; the European Council Stockholm Programme- An open and secure Europe serving and protecting the citizens 2010-2014; the Communication of the EU Commission COM (2009)262 on "An area of freedom, security and justice".

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Significant restrictions have been introduced to privacy, without giving sufficient guarantees of its re-expanding dimension as right, and the quality and effectiveness of the existing safeguards are reduced. Although all the relevant legal acts contain in general references to the need to protect HR and they often directly mention the data protection and privacy rights, the unsatisfactory level of the safeguards provided in terms of privacy and data protection have attracted many criticisms. Some examples are offered at European level (a part from the afore-mentioned Report of the UN Special Rapporteur, which offers an international overview) by the EDPS Opinions[367], by the Commitee of Regions[368], by the Art 29 Working Party[369].

It must be noted that neither the EU, nor other countries have specific regulation for the emerging AmI detection technologies: technologies such as CCTV, biometrics, Rfid, used for security purposes and which are going to be even more integrated with other technologies in an complex AmI environment[370] require a wider framework to limit the surveillance effects[371].

The entry into force of the Lisbon Treaty promises an improvement of the enjoyment of privacy and data protection rights, since many changes have been

[367] See the *Opinion of the European Data Protection Supervisor on the communication from the Commission to the EP and the Council on an Area of freedom, security and justice serving the citizen* of 10 July 2009, a relevant contribution of the EDPS to the general debate in these fields. The European Supervisor notes, in particular, that the special emphasis after the terrorist attacks was on more intrusive measures, without discussing with the same urgency the guarantees for the protection of personal data. He calls for a reflection on the consequence for European citizen before new instruments are adopted; it is important –he underlines- that the policies and intruments adopted in the Area of freedom, security and Justice should not foster the gradual move towards a surveillance society, but fully respect the citizen's fundamental rights, since "this is an area which shapes the citizen's circumstances of life, in particular the private sphere of their own responsibility and of political and social security". Express reference has been made to the recent Judgment of the German Constitutional Court of the 30 June 2009 relating to the Lisbon Treaty. Moreover, taking into account the perspective of the exponential growth of digital information on the citizen, he points out that the so-called Internet of Things and ambient intelligence are developing fast, with the consequence that digitalised characteristics of the human body (biometrics) are increasingly used: "this leads to an increasingly connected world in which public security organizations may have access to vast amounts of potentially useful information, which can directly affect the life of the persons concerned.[…] The mere fact that is technically possibile to exchange digital information between interoparable databases or to merge this data does not justify an exception to the purpose limitation principle" (Opinion EDPS, p. 19).

[368] Similar considerations made by the EDPS on the need of a comprehensive data protection scheme and of a strategic approach (based on 'privacy by design' and privacy aware techologies) to be adopted putting in place the Stockholm programme, have been expressed by the Commette of the Regions, in its Opinion of 5 and 7 October 2009 on the Stockholm programme, CONST-IV-025.

[369] See Art 29 WP and WP on Police and Justice, *Future of Privacy, Joint Contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168 of the 01 Dicember 2009, chapter 8, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

[370] Some are already in use or are object of international projects, see: http://www.riseproject.eu/ and http://www.cssc.eu/projects.php?stato=1.

[371] De Hert (2008b), *cit*., p. 73.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

introduced within the EU framework: first of all the abolition of the Pillar structure, "which, over the years, led to many questions relating to data protection"[372] and the creation of a new legal basis for data protection (art 16 of the TFEU)[373].

In particular the context of the criminal matters (former III pillar), "an area of specific concerns [for privacy and data protection], has changed with the Lisbon Treaty"[374]; the latter opened up for a comprehensive privacy and data protection framework (applicable to all processing activities).

The adoption of the European Council Framework Decision on data protection in criminal matters, although generally considered a first step towards this framework, has shown its limits against the increase of storage and exchange of personal data in relation to activities of police and justice sector. Its provisions do not have general application and do not seem to solve the problem of different application among the MS. In particular they do not apply to internal situations, when personal data originate from MS which use them, but only to the exchanges of data among MS authorities. Moreover, its essential provisions are considered by the Art 29 Working Party inconsistent with the Directive 95/46/EC[375].

For these and other reasons, a new general framework is needed, which possibly replaces the Council framework decision 2008/977/JHA with additional rules for data protection in the criminal sector[376].

Apart from the general relevance of having granted legal grounds to the fundamental right of data protection as a consequence of the adoption of Lisbon Treaty[377], at least, other two important factors deserve mention: 1) the renewed role of the European Parliament in the decision process, (as recently shown in relation to

[372] EDPS, Newsletter No 22, 12 Dicember 2009.

[373] Art 16 of TFEU states: "(1)Everyone has the right to the protection of personal data concerning them. (2)The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, officies and agencies and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. (3)Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this article shall be without prejudice to the specific rules laid down in art 39 of the TEU."

[374] Art 29 WP, *The Future of Privacy*, *cit*, p. 4.

[375] European Council Framework Decision 2008/615/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008. See the Opinion of the EDPS *cit*. (note 367), in which the Framework Decision is considered not fully satisfactory and where it is recommended to replace it, for a new more comprehensive legislative framework.

[376] *Ibid*.

[377] The new legal basis (Art 16 of TFEU), wich extends the horizontal effect across all the areas of the former 'pillars', now "obliges us to update the legal framework on data protection", as stressed out by G. Buttarelli, EDPS member at the III workshop on Data Protection in International Organizations, EUI, Florence, 27-28/05/2010
http://dataprotintorg.wordpress.com/ .

the EU/US agreements on PNR and art 17 TFEU); 2) the binding nature of the Charter of Fundamental Rights of Nice (which contains two specific provisions for privacy and data protection).

This binding effect could be particularly relevant for privacy and data protection in public security context, sector traditionally not covered by the DP Directive (former III Pillar)[378] and constituting legal exception to the privacy right (*ex* Art 8 (2) ECHR).

Thus, it can be argued that, even in the absence of a specific EU regulation addressing the processing of personal data for security reasons, some protection may be obtained through the recognition of the binding value of the EU Charter of Fundamental Rights, and consequently its applicability in contexts traditionally excluded by the Data Protection Regulation system or in which the right to privacy is limited, (art 8 (2)ECHR). It can be asserted that it is possible to assign to this Charter a 'horizontal effect' on the European law area, an effect similar to other HR instruments on International Law[379].

On a practical level, a relevant set of legal safeguards needs to be mentioned, which, working as international best practices, can help states around the world (i.e., also the European ones) to assess the necessity, proportionality and reasonableness of their security measures; these safeguards have been identified by the UN Special Rapporteur on the protection of HR while countering terrorism in the following principles: 1) *minimal intrusiveness* – requiring the exhaustion of less intrusive techniques before resorting to others; 2) *purpose specifications restricting secondary uses* – in order to limit the exceptions to purpose limitation for national security aims; 3) *oversight and regulated authorization of lawful access* - against the trend to allow law enforcement agencies to self-authorize access to personal data; 4) *transparency and integrity* – in order to ensure adequate scrutiny of surveillance systems, often based on data-mining profiles; *effective modernization* – beside the modernization of surveillance practices, there is a need for a new safeguard regime, that could benefit from 'Privacy Impact Assessments' by States)[380].

[378] As a consequence of the Pillar structure, law enforcement bodies, such as Eurojust, were not covered by the 45/2001 Regulation and did not fall under the EDPS supervision. This is another aspect that is going to change with the Lisbon Treaty.

[379] Kamminga, M. T. - Sheinin M. (2009). *The impact of Human Rights Law on General International* Law. Oxford: Oxford University Press.

[380] Report of the Special Rapporteur A/HRC/13/37, *cit*., p. 18. Other important role for the practical implementation of the privacy and data protection rules will be played by the so called *Compliance Management Systems* (CMS), as argued by the EDPS at the 'Data Protection Conference', European

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

These principles also appear to be best legal practices for future *AmI security scenarios*, where, therefore, they should be considered as a means to assess *AmI detection technologies*: as seen above, the 'softness' and 'smartness' of some technologies make them particularly suitable to be used for surveillance purposes. After all, law enforcement is a sector where effective protection should be provided against ICT threats, but also through ICT tools [381].

Technological tools for the privacy and data protection rights are particularly encouraged in the new context, especially if they can allow for the embedding these rights in the entire cycle of the technology itself, according to 'privacy by design', in order to have a regulation from 'inside' the technology not only from 'outside'[382] (e.g., eliminating automatically personal data, preventing unnecessary processing, enhancing individuals' control over their data) and 'privacy by default' approaches - privacy-protecting tools should become binding and if it is not possible to regulate all the technologies, it should be provided for at least a clear framework in which these can operate [383].

The adoption of this approach, 'embedded' in policy-making, is especially relevant in the view of realising an Ambient Intelligence world, in which the law and technology should learn from each other: legal concepts may be conceived as a *cognitive technology* [384] and automatic computation may be seen as a new script of the law, of *Ambient Law* [385].

University Institute, Florence, 27/05/2010, who pointed out the increased focus on the *accountability* principle that accompanies the updating of the DP framework.

[381] See EDPS *cit supra* note 369.

[382] See A. Montelero, Digital privacy. Tecnologie conformate e regole giuridiche, in F. Bergadano, A. Montelero, G. Ruffo, G. Sartor, *Privacy digitale, giuristi e informatici a confronto*, Giappichelli, 2005, p. 44.

[383] See the Opinion of the EDPS on promoting Trust in the Information Society by fostering Data protection and privacy, of the 19/03/2010, one of the first document of the EU after Lisbon starting with "having regard to the TFEU art 16 and[…]to the Charter of Fundamental rights art 7 and 8". One approach is particularly recommended in the Opinion in order to promote privacy by design: the promotion of a legal obligation for the producers and users of information system to use systems in accordance with this approach: the Commission should include a general provision on privacy by design in the legal framework for data protection. Nevertheless, privacy by design could not be considered a panacea for all the problems; other issues can also arise, such as who should define and how should the technical-legal rules be defined. Besides a clear framework, it is necessary to focus on the implementation of the legal principles; but in order to be confident in new protection tools we must critically evaluate them.

[384] G. Sartor, *Legal Reasoning: A Cognitive Approach to the Law*, Springer, Berlin, 2005.

[385] In response to the AmI menaces, Hildebrandt (in M. Hildebrandt & S. Gutwirth (2008), *cit*. p. 303, urges the need to re-design the technological infrastructure: in particular, as seen above, she advocates an 'ambient-law', a technological embodied law that can provide a mix of flexibility and rigidity within an AmI environment. As discussed *supra*, she suggests in particular, the inegration of PET with TET, transparency being the better mode of enpowerment of the subject: *Transparency Enhancing Technology* tools are needed in order to allow access the profiles that may be applied and can integrate the law (written administrative law, with its limits in terms of application): "what we need is an intelligent interplay between technological design and legal resolution […]the challenge is

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Notwithstanding the technological development, the law will continue to play a central role in a 'democratic society'. If the law is understood "as an *artefact*, designed taking into account a particular reality that it intends to regulate, it will be natural to think of the necessity of adapting it if the reality changes"[386].

It remains to be seen how the law will change as technology moves closer to a total pervasive environment[387], but the law should still regulate new technologies, for the reason that they have impact on the individual and social dimensions of our private life[388].

To conclude, though it could be premature to define the effects of the enforcement of the Lisbon Treaty at a European level, as far as privacy and data protection are concerned, at least one relevant benefit seems to be obtained: the constitutional efficacy of the Charter of Fundamental Rights of Nice and its horizontal effect. The latter must be taken into account from now on, when implementing (or defining) general or specific rules (also in new AmI environments).

As mentioned earlier, privacy, passed from being a mere legal term in the last centuries to being recognized as a fundamental right in many international legal instruments. Often, privacy and the underpinned values (first of all human dignity) have been challenged by the different technologies emerging over time. Today it is the turn of the network technologies, smart devices, biometric systems databases that undermine this right, since they facilitate the storage, processing and exchange of personal data by security agencies and businesses[389].

Privacy is still defined and valued by people differently and differently weighted against other values, such as public security, and possibly this uncertainty makes more urgent not only the need for multidisciplinary analysis but also for a re-conceptulization of privacy in order better to understand how new technologies

---

how to integrate these two aspects of our shared world". An intermediary solution between PET and TET has been suggested by M. Gasson *et al*. Towards a data-mining *de facto* standard, in M. Hildebrandt & S. Gutwirth (2008), *cit*., p. 58: in order to prevent the negative consequences due to possibile misuse of software tools, they suggest developing an industry standard for data-mining process, that would guide the application of software in the same way the manufacturer's instructions of electronical power-tools aim at preventing inappropriate usage. The main problem, also for technologies such as privacy- preserving data-mining, is the lack of standardization that render them ineffective for a wide application: *Ibid*. p. 86.
Since, as stressed by the EDPS, the focus in the 'Digital Agenda' will be hereinafter to enhance transparency and accountability, it appears that TETs could be useful also for a lawful deployment of *detection technologies*.

[386] M. Fernandez *et al*., *cit*., p. 28, 43.
[387] J. Ridges, *cit*., p. 751.
[388] M. Hildebrandt (2008b), *cit*. p. 311.
[389] M. Friedewald *et al.* (2010) *cit*. p. 61-67.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

impact on it and, therefore, identify privacy issues arising from dissimilar technologies.[390]

It can be noted with S. Rodotà (former President of the Italian DP Authority), that, if privacy is the foundation of citizenship, we must remember that we are dealing with real citizenship not only a digital citizenship [391].

Further studies should be conducted in order to find suitable and modern safeguards for privacy and related rights in parallel with the developments of AmI technologies and their diffused use. In an AmI world, the law, nevertheless, should still play the role of ensuring respect for fundamental values and rights, without which 'democratic society' would be no more than empty words.

[390] This is also the scope of the new PRESCIENT project, recently funded by European Commission, that considers privacy a central element in the global governance of science and technology. it aims at generating appreciation for the ethical, social, political meaning of privacy and tries to promote a social dialogue on the balance between privacy and government rights. See M. Friedewald *et al. cit.* p. 61. The project includes studies of different emerging technologies (including localization technologies, smart surveillance and biometrics) in order to identify possible privacy problems other than those falling within the taxonomy of Solove. New research directions should take the premises from this analysis. This paper, focusing on the risks for privacy deriving by AmI security scenarios, wants to be a step in this direction.

[391] S. Rodotà, speech at the III workshop on Data Protection in International Organizations, EUI, Florence, 27/05/2010.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

REFERENCES

- Aarts, E. - Encarnacao, J. (2006). *True Visions: the emergence of Ambient Intelligence*. London, Springer – Verlag.
- Aarts, E. - Marzano, S. (2003). *The New Everyday. Views on Ambient Intelligence*. Rotterdam: 010 Publishers.
- Andronikou V. et al. (2008) *Biometric profiling: opportunites and risks,* in M. Hildebrandt & S. Gutwirth (eds) *Profiling the European citizens*, London, Springer.
- Anrig, B. - Browne, W. et al. *The role of algorithms in profiling*, in M.Hildebrandt & S. Gutwirth (eds), *Profiling the European citizens*, London, Springer.
- Art 29 WP and WP on Police and Justice, *Future of Privacy, Joint Contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168 of the 01.12.2009.
- Art 29 WP, Consultation *The impact of the use of body scanners in the field of aviation security on human rights, privacy, personal dignity, health and data protection*, of the 11.02.2009.
- Art 29 WP, *Opinion 2/2004 on the Adequate Protection of Personal data contained in the PNR of Air Passengers to be transferred to the U. S. Bureau of customs and border protection*, WP 87 of the 29. 01.2004.
- Art 29 WP, *Opinion 5/2010, WP 175, on the Industry proposal for a privacy and data protection impact assessment framework for Rfid applications*, of the 13.07.2010.
- Art 29 WP, *Working document on biometrics*, WP 80 of the 01.08.2003.
- Augusto, J. (2007). Ambient Intelligence: the confluence of pervasive computing and artificial intelligence, in A. Schuster (ed). *Intelligent computing everywhere.* London, Springer- Verlag.
- Barelli, S. Casting light on the black legal hole: International law and detentions abroad in the 'war on terror', *International Review of Red Cross*, n. 857.
- Bellanova, R. & de Hert P. (2010) Le cas S. et Marper et les données personnelles, *Cultures et conflicts*, n. 76, Harmattan.
- Bennet et al. *Privacy impact assessment: international study of their application and effects report for the Information Commissioner's Office*, London Linden Consulting, 2007 available at http://www.ico.gov.uk.
- Bianca, C. M. - Busnelli, F. (2007). *La protezione dei dati personali*. Padova, Cedam.
- Bibas, S. (1994). A contractual approach to Data Privacy. *Harvard Journal Law and Public Policy* 17, 591.
- Bocca, G. "Intelligence double face", L'espresso, 22.07.2010.

- Boisson de Chazournes L. (2009). New Technologies, the precautionary principle and public participation, in Murphy T. (ed) *New technologies and Human Rights*, Oxford, Oxford University Press.
- Bosker, B. *Body Scan images from security checkpoints were saved by Feds*, Huffington Post, 04.08.2010.
- Botta, M. & Viola de Azevedo Cunha M. (2010), La protezione dei dati personali nelle relazioni tra UE e U.S.A: le negoziazioni sul trasferimento dei PNR, *Diritto dell'informazione e dell'Informatica*, Giuffrè, Milano, vol. 26, n. 2.
- Bowling, B. - Marks A. - Murphy C. (2008), *Crime Control Technologies*, in R. Brownsword, K.Yeung, *Regulating technology* (eds.) Oxford Hart Publishers.
- Brownsword, R. (2008) Knowing me, Knowing you- Profiling and the public interest in M. Hildebrandt & S. Gutwirth (eds) *Profiling the European citizens*, London, Springer.
- Brownsword, R. (2008), Knowing me, Knowing you-Profiling, Privacy and the Public interest, in M. Hildebrandt & S. Gutwirth (eds) *Profiling the European citizen*, London, Springer.
- Buttarelli, G. (1997). *Banche dati e tutela della riservatezza,* Milano, Giuffrè.
- Bygrave, L. (2008). International agreements to protect personal data. in J. B. Rule- G. Greenleaf (ed), *Global Privacy Protection*, Cheltenham: Edwar Elgar Publishing.
- Canhoto, A. and J.Backhouse (2008), General description of the process of behavioural profiling, in M. Hildebrandt & S. Gutwirth *Profiling the European citizen*, London, Springer.
- Casanovas, P. The future of Law: Relational Justice, Web Services and Second-generation Semantic Web, in M. Fernandez-Barrera et al.(2009) *Law and technology. Looking into the Future,* European Press Academic Publishing.
- Clarke R. (2009) Privacy Impact Assessment: its origin its development, *Computer Law and Security Review*, vol. 25, 2.
- Clements, B. I. Maghiros, L. Beslay, et al. (eds), 2003, Report on *Security and privacy for the Citizen in the post- September 11 Digital Age. A prospective overview*, European Commission, IPTS-Report Series, EUR 20823.
- Cohen, J. E. (2000). Examined Lives: Informational privacy and Subject as Object*, Stanford Law Review*, 52, 1373.
- Cook. D. - Augusto J. C. et al. (2009). Ambient Intelligence: Technologies, applications and opportunities. *Pervasive and Mobile Computing*, 5 (4), 277-298.
- Cremona, M. - De Witte B. (2008). *EU foreign relations law: constitutional fundamentals*, Oxford: Hart.
- Daskala B. - Maghiros, I. (2007). *Digital Territories: towards the protection of public and private spaces in a digital and Ambient Intelligence environment*, (IPTS Report), Luxemburg: OPOCE.

- De Beer, D. - De Hert, P. - Gonzalez Fuster, G. - Gutwirth S. (2010), Nouveax Eclairages de la notion de "donnés personnelle" e application audacieuse du critère de proportionnalité, *Revue Trimestrielle droits de l'homme* (81/2010), Bruxelles, Bruylant.
- De Hert P. & Gutwirth S. (2009) Data Protection in the case law of Strasbourg and Luxembourg: Constitutionalization in Action, in S. Gutwirth et al. (eds.) *Reinventing Data Protection?* London, Springer.
- De Hert, P. & Gutwirth S. (2006) Privacy, Data Protection and law enforcement. Opacity of the individual and transparency of power, in E. Claes, et al. *Privacy and the criminal law*, Antwerp, Intersentia.
- De Hert, P. (2005), Balancing Security and Liberty within the European Human Rights Framework: A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11. *Utrecht Law Review* 1(1), 68-96.
- De Hert, P. (2008b), Identity management of e-ID, privacy and security in Europe. A human rights view*, Information Security technical Report*, 13.
- De Hert, P.(2008a) The use of labour law to regulate employer profiling: making data protection relevant again, in M. Hildebrandt & S. Gurtwirth (eds.) *Profiling the European citizen*, London, Springer.
- De Vries, K. - Bellanova R. & De Hert P. (2010) Proportionality overrides unlimited surveillance, *CEPS, Liberty and Security in Europe*/May 2010 available at http://www.vub.ac.be/LSTS/pub/Dehert/342.pdf.
- De Vries, K. (2010). Identity, profiling algorithms and a world of ambient intelligence, *Ethics and Information Technology*, 12 (1).
- Dix, A. (2005). Le tecniche Rfid in G. Rasi (ed) *Innovazioni tecnologiche e privacy*. Rome, Ufficio grafico dell'Istituto Poligrafico e Zecca dello Stato.
- Dreyer, E. (2005). Le respect de la vie privée objet d'un droit fondamental, *Lexis-Nexis Juris- Classeur* 5 (18).
- Ducatel, K. et al. (2001). Scenarios for Ambient Intelligence in 2010, EUR 19763, EC-JRC, IPTS, Seville, from: http://cordis.europa.eu/fp7/ict/istag/home_en.html.
- EDPS (2009), *Opinion on the Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee towards a European e-Justice Strategy, Official Journal of the European Union (2009/C 128/02).*
- *EDPS Opinion on the communication from the Commission to the EP and the Council on an Area of fredom, security and justice serving the citizen* of 10.07.2009.
- EDPS, Opinion on *Promoting Trust in the Information Society by fostering data protection and privacy* of 18.03.2010,
- EPIC (Electronic Privacy Information Center), *Whole Body Imaging Technology and body scanners,* http://epic.org/privacy/airtravel/backscatter/.

- Etzioni A. (2002), Implication of Select new technologies for individual rights and public safety, *the Harvard Journal of Law and Technology*, vol 15, n. 2.
- Etzioni A. (2004) DNA tests and databases in Criminal Justice: individual rights and the common good in D. Lazer (eds.) *DNA and the Criminal Justice system: the technology of Justice*, MIT Press.
- European Fundamental Rights Agency (FRA), 2010, *Data Protection in EU: the role of National Data Protection Authorities – Streinghtening the fundamental rights architecture in the EU II*, available at http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf.
- European Fundamental Rights Agency (FRA), 2010, *The use of body scanners. Ten questions and answers of the 10 July 2010*, Luxemburg: publications office of the European Union.
- European Commission *Communication Rfid, Steps towards a policy framework* (COM (2007) 96), http://ec.europa.eu/information_society/policy/rfid/documents/infso_com_2007_96.pdf.
- European Commission Communication on An area of freedom, security and justice (COM (2009)262) of 10 June 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0262:FIN:EN:PDF .
- European Commission Communication to the EP, the Council, the EESC and the Commitee of the Regions on Internet of Things – An action plan for Europe (COM (2009) 278) of the 18.06.2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:HTML.
- European Commission, Communication from the Commission to the European Parliament and the Council on the use of the security scanners at the EU airports, COM (2010) 311/4 of the 15 June 2010, http://ec.europa.eu/transport/air/security/doc/com2010_311_4_security_scanners.pdf .
- European Commission, Communication on the follow-up of the Work program for better implementation of the Data Protection Directive, COM (2007) 87 final, of the 07 March 2007, http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf
- Fernandez-Barrera, M. et al. (2009). *Law and Technology: Looking into the Future*. Pistoia: European Press Academic Publishing.
- Forsythe, D. P. *Human Rights Studies. On the dangers of legalistic assumptions*, Intersentia,
- Friedewald, M. - Vildjiounaite, E. et al. (2007). Privacy, identity and security in ambient intelligence: a scenario analysis. *Telematics and Informatics*, 24 (1), 15-29.
- Friedewald, M. - Wright, D. Gutwirth, S. Mordini, E., Privacy, data protection and emerging sciences and technologies: towards a common framework, *The European Journal of Social Science Research*, vol. 23, n.1, 2010.

- Gandy O. H. & Schiller H. (2002), *Data Mining and surveillance in the post-9.11 environment*, IAMCR, Barcelona.
- Gasson M. et al. (2008), Towards a dataming de facto standard, in M. Hildebrandt & S. Gutwirth (eds) *Profiling the European citizens*, London, Springer.
- Guarda, P. (2009) The Myth of Odin's Eye: privacy vs Knowledge, in M. Ferndandez-Barrera et al., *Law and Technologies: Looking into the future*. Florence, European Press Academic Publishing.
- Guelke J. & T. Sorell, *Detection Tecnology Survey n. 5* for the DETECTER project - D12.2.5 of the 02.06.2010, available at http://www.detecter.bham.ac.uk/.
- Gutwirth S. & De Hert P. (2008), Regulating profiling in a democratic constitutional state, in M. Hildebrandt & S. Gutwirth (eds) *Profiling the European citizen*, London, Springer.
- Gutwirth S. et al. (eds.) 2009, *Reinventing Data Protection?* Springer, London.
- Gutwirth, S. (2007). Biometrics between opacity and transparency, *Annuali dell'Istituto superiore di Sanità*, 43 (1), 61-65.
- Hildebrandt, M. & Gutwirth S. (eds.) (2008) *Profiling the European citizen*, London, Springer.
- Hildebrandt, M. (2005). Privacy and Identity, in E. Claes - A. Duff - S. Gutwirth, *Privacy ad the criminal Law*. Antwerp- Oxford: Intersentia.
- Hildebrandt, M. (2008a) *Profiling and the rule of law*, Identity in the Information Society, London, Springer.
- Hildebrandt, M. (2008b) Defining profiling. A new type of Knowledge in M. Hildebrandt, S. Gutwirth (eds.) *Profiling the European citizen*, London, Springer.
- Hildebrandt, M. (2008c), Legal and technological normativity: more (and less) than twin sisters, *Techné: research in philosophy and Technology,* 12.
- Hildebrandt, M. (2010), *A vision of Ambient Law*, in R. Bronwsword & K Yeung, *Regulating technologies.*
- Hildebrandt, M. Makinwa, Foehmichen. A. (eds.), 2009, *Controlling Security in a Culture of fear*, The Hague, BJU, Legal Publishers.
- Hoikkaanen, A. - Bacigalupo, M. - Compano, R. - Lusoli, W. - Maghiros, I. (2010). New challenges and possible policy options for the regulation of electronic Identity, *Journal of International Commercial Law and Technology*, 5 (1).
- Jaquet-Chiffelle, D. O. (2008), *Direct and indirect profiling in the light of virtual persons*, in M. Hildebrandt & S. Gurtwirth (eds.) *Profiling the European citizen*, London, Springer.
- Joinson A. N. et al. (2006). The role of situational and dispositional variables in online *disclosures*. Paper presented at the Workshop on Privacy, Trust and Identity Issues for Ambient Intelligence. from: http://www.cs.st-andrews.ac.uk/~pst/pti-ai-workshop/programme/joinson-privacy.pdf.

- Kamminga, M. T. - Sheinin M. (2009). *The impact of Human Rights Law on General International* Law. Oxford: Oxford University Press.
- Keats Citron, D. - Henry L. M. (2010). Visionary Pragmatism and the value of privacy in the Twenty-first century. *Michigan Law Review*, 108, 1107.
- Kindt E. (2008) Need of legal analysis of biometric profiling in M.Hildebrandr & S. Gutwirth, (eds) *Profiling the European citizen*, London, Springer.
- Koops B.J. & Prinsen M. (2007), Houses of Glass, Transparent Bodies: how new technologies affect inviolability of hte Home and Bodily Integrity in the Dutch Constitution, *Information & Communications Technology Law*, Vol. 16, n. 3, Routledge.
- Koops, B.-J. (2008), Some riflection on profiling, in Hildebrandt & S. Gutwirth (eds.) *Profiling the European citizen*, London, Springer.
- Kosta, E. - Zibushka, J. Scherner, T. -Dumortier J. (2008). Legal considerations on privacy-enhancing Location Based Services using PRIME technology. *Computer Law and Security Report* 24 (2).
- Le Metayer D. & Monteleone S. (2009). Automated consent through privacy agents: legal requirements and technical architecture. *Computer Law and Security Review*, 25 (2), 136-144.
- Le Metayer D. & Rouvroy A. (2008), *STIC et droit, conflits et complémentarités*, Interstices. Ed. INRIA Available at http://interstices.info/jcms/c_34521/stic-et-droit-defis-conflits-et-complementarites.
- Le Métayer, D. (2010). Privacy by design: a matter of choice, in Gutwirth S. et al. *Data Protection in a profiled world*. London, Springer.
- Leenes, R. - Koops, B. J. - de Hert, P. (2008). *Constitutional Rights and New Technologies. A comparative study*, The Hague, T. M. C. Asser Press.
- Leenes, R. (2008a) Addressing the obscurity of data clouds, in M. Hindebrandt & S. Gurtwirth (eds.) *Profiling the European citizen*, London, Springer.
- Leenes, R. (2008b). Do you know me? Decomposing identifiability. *Tilburg University Legal Studies Working Paper* n. 01/2008.
- Lessing, L. (1999). *The Code and other Laws of cyberspace*. New York, Basic Books.
- Lorello, M. *Debutta a Punta Raisi il body scanner "sicuro",* la Repubblica, 31.07.2010.
- Lu J-M & Wang M-J. (2008) Automated anthropometric data collection using 3D whole body scanners, *Expert System with application,* 35.
- Lugaresi, N. (2004). Protezione della privacy e protezione dei dati personali: i limiti dell'approccio comunitario, *Giustizia amministrativa* n. 03/2004. Rome, Istituto poligrafico e Zecca dello Stato.
- Lyon, D. - Zureik, E. (1996). *Computer, Surveillance and privacy*. Minneapolis, University of Minnesota Press.
- Lyon, D. (2007). *Surveillance studies, an overview*. Cambridge, Polity.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

- Marx, G. T. (2001). Technology and Social Control in N. Smalser- P. Baltes (eds) International Encyclopedia of the social and behavioral Science, Oxford, Elsevier.
- Marx, G. T. (2002), What's new about the 'New Surveillance'? Classifying for change and continuity, *Surveillance & Society*, 12.
- Marx, G. T. (2005), Surveillance and society, *Encyclopedia of Social Theory*, available at http://web.mit.edu/gtmarx/www/surandsoc.html.
- Marx, G.T. (2006), Soft Surveillance, The Growth of Mandatory Volunteerism in Collecting Personal Information, in Monahan T. *Surveillance and Security. Technological Politics and Power in everyday life*, New York/London, Routledge.
- Marx, M.T. - Steeves, V. From the beginning: children as subjects and agents of surveillance, *Surveillance and Society*, vol. 7, n. 3/4, 2010.
- Montelero, A. (2005) Digital privacy. Tecnologie conformate e regole giuridiche, in F. Bergadano, A. Montelero, G. Ruffo, G. Sartor, *Privacy digitale, giuristi e informatici a confronto*, Giappichelli.
- Monteleone, S. (2008) Data Protection e comunicazioni: necessità di un approccio tecnico-giuridico, in A. Pace, R. Zaccaria, G. De Minico, *Mezzi di comunicazione e riservatezza*, Jovene.
- Monti, A. *Italian DNA Database: the davil is in the details,* EDRI-gram n.7.16, of the 26/08/2009.
- Nabeth T. (2008) Reply to M. Hildebrandt, in M. Hildebrandt & S. Gutwirth eds) *Profiling the European citizen*, London, Springer.
- OECD Using Sensor-based Networks to address Global Issues: Policy opportunities and Challenges, Lisbon, 8-9 June 2009,
- Pop, V. *US Outstrips Europe on body scanners*, Business Week, 23.06.2010.
- Poullet, Y. (1991). Le fondement du droit à la protection des données nominatives: propriétés ou libertés*, Nouvelles technologies et propriété*. Paris : Thémis.
- Poullet, Y. (2001). Conclude a Contract through Electronic Agents? *Electronic Commerce – DER Abschlub von Vertragen im Internet*. Baden Baden: Verlagsgesellschaft.
- Poullet, Y. (2004). The fight against crime and/or the protection of privacy: a thorny debate? *International Review of Law, Computers & Technology*, 18 (2), 251-273.
- Poullet, Y. (2005d), *Directive 95/46: ten years after,* in Proceedings of the XXVII Internet Conference of the Data Protection Commissioners, Montreaux.
- Poullet, Y. (2005a). Comment réguler la protection des données? Réflexions sur l'internormativité, in P. Delnoy, *Liber amicorum*. Bruxelles, Larcier.
- Poullet, Y. (2005b). Pour une troisième génération de réglementations de protection de données, *Jusletter*, 3 (22).
- Poullet, Y. (2005c). The Internet and private life, in Kenyon and Richardson (ed) *New dimension of privacy*. Cambridge, Cambridge University Press

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

- Punie, Y. (2005). The future of Ambient Intelligent in Europe: the need for more everyday life in R. Silverstone (ed) *Media, technology and everyday life in Europe: from Information to Communication*. London: Ashgate Publishers Ltd.
- Report (2009) of the UN Special Rapporteur on the promotion and protection of HR and fundamental freedoms while countering terrorism *A/HRC/13/37*.
- Ridges J. (2008), What happens when everything becomes connected: the impact on privacy when technology becomes pervasive, *49 South Texas Law Review*.
- Roach. K. (2006), Must we trade rights for security? The choice between smart, harsh, or proportionate security strategies in Canada and Britain, *27 Cardozo Law Review*.
- Rodotà, S. (1997). *Repertorio di fine secolo.* Roma, Laterza.
- Rodotà, S. (2009). *La vita e le regole, tra diritto e non diritto*. Milano, Feltrinelli.
- Rouvroy A. & Berns T. (2009), *Détecter et prévenir: de la digitalisation des corps et de la docilité des normes*, in L. Guy- J. Mariau (eds*.) Gouverner par les corps*, P.I.E. Peter Lang, (forthcoming).
- Rouvroy, A. (2008b) Réinventer l'art d'oublier et de se faire oublier dans la seciété de l'information? In S. Lacour (Ed.), *La sécurité de l'individue numerisé*, Paris, L'Harmattan.
- Rouvroy, A. (2008a). Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence*, Studies in Ethics, Law, and Technology*, 108 (2).
- Rouvroy, A. (2009), Le corps statistique, *La Pensée et les Hommes,* n.74, ed. P. Deled, available at http://works.bepress.com/antoinette_rouvroy/29/.
- Rouvroy, A. (2010a) *Governamentality in an Age of Autonomic Computing: Technology, Virtuality and Utopia*, in M. Hildebrandt, A. Rouvroy (eds.), *Autonomic Computing and the Transformation of Human Agency. Philosophers of Law meet Philosophers of Technology*, Routledge.
- Rouvroy, A. (2010b), Detecter et prevenir, Les symthomes technologiques d'une nouvelle manière de gouverner, *Etat des droits de l'Homme en Belgique*, Brussels, Aden.
- Sartor, G. & Viola de Azevedo Cunha, M. (2010). The Italian Google-Case: Privacy, Freedom of Speech and Responsibility for User-Generated Contents, *Social Science Research Network*, Working Papers.
- Sartor, G. (2006). Privacy, Reputation and Trust: some implications for Data Protection, *EUI Working Papers*, Law n. 2006/04, Florence, European University Institute.
- Sartor, G. (2005) *Legal Reasoning: A Cognitive Approach to the Law*, Springer, Berlin.
- Schreurs, W. et al. (2008), *Cogitas, Ergo Sum. The role of data protection Law and non-discrimination law in group profiling in the private sector*, in M. Hildebrandt & S. Gurtwirth (eds.) *Profiling the European citizen*, London, Springer.
- Sheinin M. et al. (2009). Law and Security. Facing the dilemmas. *EUI working papers Law* 2009/11. Florence: European University Institute.

- Sheinin, M. & Vermeulen M. (2010), Unilateral exceptions to international law: systematic legal analysis and critique of doctrines that seek to deny or reduce the applicability of human rights norms in the fight against terrorism, *EUI Working papers, Law 2010/08*, Florence, European University Istitute.
- Simpson R. et al. (2006). Plans and Planning in Smart homes, in J. Augusto - C. Nugent. *Designing Smart Homes*. *The role of Artificial Intelligence*, London, Springer- Verlag.
- Solove D. (2007). "I've got nothing to Hide" and other misunderstandings of Privacy, *San Diego Law Review.*
- Solove, D. (2008). *Understanding Privacy*, Harvard: Harvard University Press.
- Solove, D. (2004). *The Digital Person. Technology and privacy in the Information Age*, New York, NY University Press.
- Steinbock, D.J. (2005) *Data Matching, data mining* Georgia Law Review, vol. 40, 1.
- Stranieri, A. & Zeleznikow J. (2005) Knowledge *Discovery from Legal Databases*, Springer.
- Sudre, F. (2005). La "construction" par le Juge européen du droit au respect de la vie privée, in F. Sudre, *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*. Brussels, Bruylant.
- Van Bendegem, J. (2008) Neat Algorithms in messy environments, in M. Hildebrandt & S. Gutwirth (eds) *Profiling the European citizen*, London, Springer.
- Van der Hof & Prins, *Personalization and its influence on identities, behaviour and social values*, in M. Hildebrandt & S. Gurtwirth (eds.) *Profiling the European citizen*, London, Springer.
- Van Der Schyff, G. (2005) *Limitation of rights,* Wolf Legal publisher, Nijmegen.
- Van Dijk, N. Property, Privacy and Personhood in a world of Ambient Intelligence, *Ethics and Information techologies*, Issue 1, vol. 12 Springer.
- Van Ooijen C. & Soeparman S. (2010) *Surveillance in a State of Precaution. A discourse mediating state control and sociability*. Paper presented to the 'Challenging the Panopticon Effect' Conference, london, 13-15.04.2010.
- Vermeulen, G. & W.De Bondt, (2008) Finding the right balance between effective measures and fundamental rights guarantees, 79 *Revue internationale de droit penal*.
- Vildjiounaite E. - Makea, S.M.- Lindholm, M. - Rihimaki, R. et al. (2006). Unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices, in *Pervasive Computing*, Proceedings of the 4th International Conference, PERVASIVE 2006, Dublin, Ireland, May 7-10, 2006. Berlin-Heidelberg, Springer.
- Warren S. & L. Brandeis (1890). The Right to Privacy. *Harvard Law Review,* 4 (5).
- Weyembergh M. (2002), Le Problème, in E. Bribosia, A. Weyembergh, *Lutte au terrorisme et droits fondamentaux*, Bruxelles, Bruylant.

Monteleone, Shara (2010), Ambient Intelligence and the Right to Privacy. The challenge of detection technologies
European University Institute DOI: 10.2870/24183

- Wright D. - Gurtwirth, S. et al. (2008). *Safeguards in a world in Ambient Intelligence*, London, Springer.
- Wright D. - Gurtwirth, S. et al. (2009). Privacy, trust and policy-making: challenges and responces. *Computer Law and Security Review*, 25 (1), 69-83.
- Wright D. (2005). The dark side of AmI. *The Journal of policy, regulation and strategies for Telecommunications* 7(6).
- Yannopoulos, A. et al. Behavioural biometric profiling and Ambient Intelligence, in Hildebrandt & S. Gutwirth (eds.) *Profiling the European citizen*, London, Springer.
- Zucca L. (2008). *Constitutional Dilemmas*. Oxford, Oxford University Press.